UNIVERSIDAD CARLOS III DE MADRID

TRABAJO FIN DE GRADO

ESTUDIO DEL RENDIMIENTO BIOMÉTRICO DE SISTEMAS DE HUELLA DACTILAR. ANÁLISIS DE DIFERENTES SENSORES Y ALGORITMOS

GRADO EN INGENIERÍA ELECTRÓNICA INDUSTRIAL Y AUTOMÁTICA

Autor: Sergio Sánchez Martín

Tutor: Raúl Sánchez Reíllo

Leganés, 25 de septiembre de 2015

RESUMEN

Este proyecto tiene como elemento principal los sistemas de reconocimiento biométrico basados en huella dactilar. Estos sistemas, son altamente utilizados e implementados en aplicaciones de todo tipo como para el control de accesos o forenses. Por lo que en este TFG se realizará una evaluación de rendimiento de un sistema de reconocimiento biométrico analizando dos algoritmos, con tres sensores de huellas basados en distintas tecnologías: uno térmico y dos capacitivos.

La realización de la evaluación se ha efectuado a partir de una base de datos obtenida durante las prácticas en empresa cursadas en el Grupo Universitario de Tecnologías de la Identificación, en la que se obtuvieron las huellas de los dedos pulgar, índice y corazón de ambas manos de 589 individuos.

El trabajo realizado ha sido el procesamiento de la base de datos desarrollando una aplicación en el entorno Microsoft Visual Studio 2013 capaz de ejecutar la comparación de las muestras obtenidas por cada sensor con cada algoritmo.

Los resultados son almacenados en diferentes ficheros, correspondientes a cada sensor y algoritmo, realizando la distinción entre genuinos e impostores.

Con un software implementado en Matlab se realiza la segunda parte del proyecto: el procesamiento de los ficheros para obtener las medidas de rendimiento gráficas del análisis realizado.

El presente documento describe el diseño y desarrollo del trabajo realizado, junto con los resultados obtenidos tras efectuar el análisis de rendimiento.

Palabras clave

Biometría, sistema de reconocimiento biométrico, huella dactilar, algoritmo, medidas de rendimiento, sensor biométrico.

ABSTRACT

This project's main focus is the biometric recognition systems based on fingerprint, which all kinds of applications take advantage of, such as control access or forensic realms. Therefore, this TFG includes a performance evaluation of a biometric recognition system, made by assessing two dedicated algorithms. Three fingerprint-based sensors, which belong to different technologies has been used: one termic and two capacitive sensors.

A Data base, generated during some internship within the "Grupo Universitario de Tecnologías de la Identificación", was the driver of the assessment. The result was a collection of fingerprints (thumb, fore finger and middle finger) from 589 different people.

Microsoft Visual Studio 2013 was the selected environment to process the Data Base by means of a purpose-built application that is able to compare per sensor and per algorithm every sample to each other. The genuine-false detections were stored in separated files, each one corresponding just to one sensor and one algorithm.

The second part of the project conceived the use of Matlab in order to produce a turnkey software module to process those files. This process produced the graphical performance measurements of the assessment.

Summarising, this document depicts the work's design and development as well as it collects the performance assessment's results.

Key words

Biometric, biometric recognition system, fingerprint, algorithm, performance measures, biometric sensor.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

LISTA DE ACRÓNIMOS

.DLL	Dynamic Link Library
a. C	Antes de Cristo
C#	C Sharp
C++	C plus plus
CCD	Charge Coupled Device
DET	Detection Error Tradeoff
dpi	Dots Per Inch
EER	Equal Error Rate
FAR	False Accept Rate
FBI	Federal Bureau of Investigation
FMR	False Match Rate
FNIR	False Negative Identification Rate
FNMR	False Non-Match Rate
FPC	Sensor huella dactilar FPC1011F3
FPIR	False Positive Identification Rate
FRR	False Reject Rate
FTA	Failure To Acquire rate
FTE	Failure To Enrol rate
GUTI	Grupo Universitario de Tecnologías de la Identificación
LED	Light Emitting Diode
MATLAB	Matrix Laboratory
MCC	Minutia Cylinder Code
NBIS	NIST Biometric Image Software
NIST	National Institute of Standards and Technology
NXT	Sensor huella dactilar NB-3010-U
ppi	Pixels Per Inch
ROC	Receiver Operating Characteristic
SDK	Software Development Kit
TFG	Trabajo de Fin de Grado
UPK	Sensor huella dactilar UPEK EikonTouch 510
WPF	Windows Presentation Foundation

CAPÍTULO 1. INTRODUCCIÓN

A diario, el ser humano realiza una acción inevitable: la identificación de otro individuo. Esta actividad se realiza de forma instintiva y continua.

Simplemente el hecho de mirar a una persona para saber si es conocida o no, ya supone una identificación. Por lo tanto el inicio de la misma está ligado al origen del ser humano y las civilizaciones.

Las pinturas rupestres en las cavernas muestran los primeros indicios de la identificación del ser humano, en las que se pueden encontrar marcas de manos en las paredes.

Con la evolución de la civilización y los conocimientos, el ser humano continuó con la búsqueda de nuevos métodos para poder identificar a cada persona. Existen documentos de transacciones comerciales en los que los comerciantes orientales firmaban con su huella dactilar.

El desarrollo evolutivo de la civilización y con él, el desarrollo tecnológico dio lugar a nuevas técnicas para realizar la identificación de forma automática, segura e inequívoca.

La biometría, en el campo de la identificación, recoge los métodos automáticos usados para analizar diferentes características humanas con el fin de identificar y autentificar a las personas. Proviene del griego: bio- (vida) y -metría (medida) [1].

Las características estudiadas pueden ser tanto físicas o estáticas (ej. Iris, huella dactilar, geometría vascular, etc.), como de comportamiento o dinámicas (ej. Firma manuscrita, tecleo, etc.), o combinación de ambas como la voz [2].

El auge de la biometría comenzó hace algunas décadas, entorno a los años sesenta. Su uso está ligado a la necesidad de las autoridades de poder identificar tanto al infractor de un delito como a la víctima del mismo. Pero también se dan múltiples ámbitos en los que la implantación de la biometría cobra una gran importancia, como es en el caso de la seguridad, especialmente cuando otras tecnologías no son suficiente. Hoy en día el uso de un sistema biométrico ya no es algo inverosímil de las películas de ciencia ficción, se puede encontrar en un banco para abrir una caja fuerte, para desbloquear un *smartphone*, para tener acceso a una zona restringida o simplemente para fichar en el puesto de trabajo.

La huella dactilar como característica para la identificación, es una de las más populares y aceptadas dado que cumple con los requisitos establecidos para poder considerarse una característica biométrica: universalidad, unicidad, permanencia, facilidad para la captura, rendimiento razonable para la identificación y aceptación por parte del usuario [2].

Existen evidencias de que en el 500 a. C los comerciantes de Babilonia incluían las huellas dactilares en las tablas de arcilla donde figuraban las transacciones realizadas [1].

En 1891 Juan Vucetich estableció el primer método de clasificación de ficheros de huellas dactilares, poniéndolo en práctica identificando al autor de un crimen gracias a las huellas encontradas en la escena del hecho, convirtiendo a Argentina en el primer país que usó la dactiloscopia (sistema de identificación basado en el estudio y comparación de las huellas dactilares) para resolver un crimen [3].

No obstante, los sistemas de reconocimiento biométrico están en constante desarrollo, buscando la perfección de los mismos, para garantizar en todo momento la fiabilidad y seguridad requerida, y así poder lograr la máxima aceptación del usuario.

1.1 Motivación y objetivos

La motivación de este proyecto surge tras la realización de las Prácticas Externas, en las cuales se produjo la adquisición de conocimientos sobre los sistemas de reconocimiento biométrico, centrándose en las huellas dactilares, y las técnicas empleadas para la captura de muestras y la creación y gestión de una base de datos.

Además, hoy en día la biometría de huella dactilar no está únicamente destinada a entornos forenses o policiales, sino que se puede encontrar en múltiples aplicaciones para todo tipo de usuarios. Buscando siempre aumentar la seguridad, y obtener un mayor grado de aceptación por parte de la sociedad.

Esta modalidad es de las primeras en ser analizadas, algunos de los factores influyentes son la fácil adquisición de las muestras, siendo una técnica no invasiva, y su largo periodo de uso e investigación sobre la misma.

El objetivo principal es realizar un análisis a través de una evaluación de rendimiento tecnológico, en el que se pretende obtener un resultado aclaratorio de la comparativa entre dos algoritmos utilizados en la modalidad de huella dactilar tras la obtención de una base de datos mediante tres sensores diferentes. La realización de este tipo de evaluación es necesaria dado que sin ella no se podría llevar a cabo otro tipo de evaluación, la de seguridad.

En este estudio se efectuará el análisis de rendimiento mediante la implementación de dos aplicaciones.

Una de ellas se encargará de realizar el procesado de la base de datos proporcionando unos resultados de comparación, los cuales serán empleados en una segunda aplicación que generará gráficos representativos, permitiendo realizar el análisis correspondiente.

1.2 Entorno socio-económico

Actualmente, gracias a la concienciación pública y la aceptación generalizada, el desarrollo de tecnologías basadas en biometría, en España, está obteniendo un continuo crecimiento.

Las grandes inversiones en esta tecnología se encuentran en las Administraciones Públicas, principalmente en proyectos destinados a Defensa y Seguridad Nacional. No obstante, sectores privados, como es el caso del financiero o el hotelero, también están desarrollando grandes proyectos en este ámbito [38].

La aplicación donde se implementan el mayor número de sistemas de identificación biométrica es en el control de accesos, tanto físicos como lógicos. En España, la modalidad más utilizada para este tipo de aplicación es la huella dactilar, debido a su alto grado de madurez, los precios competitivos y su usabilidad.

La principal ventaja en la que se sustenta el desarrollo de la biometría para sistemas de identificación, es el alto grado de seguridad que ofrecen. Por este motivo, la realización de evaluaciones de rendimiento son de alta prioridad dado que a partir de ellas es posible realizar las de seguridad.

La implantación de sistemas de identificación biométrica se prevé en aumento, tanto en el sector público como en el privado, según vaya mejorando su situación en el mercado. El desarrollo de la investigación es de gran importancia para ofrecer nuevas soluciones a las entidades y conseguir la reducción de costes, uno de los principales inconvenientes que retrasa la implementación de este tipo de sistemas [38].

1.3 Marco regulador

En este apartado se resume la normativa aplicable al uso de sistemas basados en datos biométricos.

Durante los últimos años ha aumentado el interés por elaborar estándares para el uso de sistemas biométricos, pero todavía son insuficientes y deficientes.

A nivel mundial los principales organismos que regulan la estandarización de este tipo de tecnología son: el Sub-Comité 37 del Joint Technical Committee on Information Technology (ISO/IEC JTC1), del International Organization for Standardization (ISO) y el International Electrotechnical Commission (IEC) [39].

En España, la Agencia Española de Protección de Datos (AEPD) define, en el Informe Jurídico número 0368/2006 de la AEPD sobre huella dactilar, que los datos biométricos son aquellos aspectos físicos que mediante un análisis técnico permiten distinguir las singularidades, sirviendo para identificar al individuo en cuestión [38].

Los sistemas encargados de procesar los datos biométricos deben estar reglados bajo las medidas de seguridad de carácter físico, técnico y/u organizativo de nivel básico según el Título VIII del Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos (LOPD). Si además, los datos biométricos estuviesen vinculados a la salud de los afectados las medidas de seguridad implementadas corresponden al nivel medio y alto.

En el nivel básico se definen los deberes y funciones del personal con acceso a los datos biométricos. Y en el nivel alto, que contiene el nivel medio y bajo, se debe nombrar un responsable de seguridad y se incluye la gestión y distribución de soportes, como la securización de la transmisión de datos a través de redes de telecomunicaciones [38].

Para realizar esta evaluación de forma óptima y repetible, se trabaja bajo la normativa ISO/IEC 19795, la cual proporciona las reglas y recomendaciones para efectuar correctamente una evaluación de estas características, es decir, tecnológica.

1.4 Estructura del documento

Este documento se estructura en seis capítulos.

El primero corresponde a la introducción general, donde se expone un primer contacto con el tema principal, la motivación y los objetivos del proyecto, el entorno socio-económico y regulador en España, además de la estructura que sigue la memoria.

En el segundo capítulo se encuentra el estado del arte de esta tecnología, organizado en subapartados en los que se explica qué es:

- La biometría junto con sus principales características, modalidades, sistemas de reconocimiento biométrico, evaluación de los mismos y medidas del rendimiento.
- La huella dactilar y las características de los sistemas biométricos en esta modalidad.
- Los sensores de huella dactilar ya sean ópticos, térmicos, capacitivos y/o mecánicos.

El tercer capítulo hace referencia a la explicación del diseño del estudio dividiéndose en:

- El análisis de rendimiento tecnológico de un sistema biométrico de huella dactilar.
- Los algoritmos a analizar.
- La descripción de la base de datos empleada.
- La descripción de los requisitos de la aplicación implementada para realizar la comparación.
- La descripción de los requisitos de la aplicación implementada para la obtención de los resultados gráficos.

En el cuarto capítulo se expone el desarrollo seguido para alcanzar los objetivos marcados en el proyecto. Dividiéndose en:

- Descripción del desarrollo de la aplicación de la comparación y su funcionamiento.
- Descripción del desarrollo de la aplicación para la obtención de los resultados gráficos y su funcionamiento.

El quinto capítulo corresponde a la presentación de las medidas de rendimiento obtenidas en forma de gráficas y tablas, seguido de su correspondiente análisis.

Estas gráficas se dividen por sensores y curvas analizadas, para los distintos algoritmos.

Además contiene una comparativa en la que aparecen las curvas para los tres sensores en la misma gráfica, para poder obtener una representación visual de la comparación.

El último capítulo incluye las conclusiones obtenidas tras la realización del proyecto y las líneas de trabajo futuras.

CAPÍTULO 2. ESTADO DEL ARTE

En el presente capítulo se aporta la situación actual de la tecnología empleada en este estudio: la biometría. Explicando en distintos apartados, cada uno de los aspectos que la componen, como son las características, las modalidades, los sistemas de reconocimiento, la evaluación de dichos sistemas y las medidas de rendimiento.

Además, se incluyen distintos apartados destinados a la explicación de la modalidad empleada en este proyecto: la huella dactilar.

2.1 Biometría

En el campo de la identificación se entiende por biometría al reconocimiento automático de individuos por medio de sus rasgos físicos o de comportamiento [2]. Estos rasgos suelen ser denominados características biométricas.

Como ya se comentó en el Capítulo 1, el auge de la biometría comenzó hace algunas décadas, entorno a los años sesenta. Su uso está ligado a la necesidad de las autoridades de poder identificar tanto al infractor de un delito como a la víctima del mismo. Pero también se dan múltiples ámbitos en los que su implantación cobra una gran importancia, como es en el caso de la seguridad, especialmente cuando otras tecnologías no son suficiente.

2.1.1 Características biométricas

La identificación, o reconocimiento, se realiza mediante el análisis de las características biométricas las cuales deben cumplir los siguientes requisitos [2]:

- Universalidad: todo individuo debe poseerla y por tanto puede usarla.
- Unicidad o singularidad: debe ser única para cada individuo siendo diferente del resto.
- Permanencia: no puede ser efímera, es decir, debe permanecer constante e inmutable en el tiempo.
- Facilidad en la adquisición: la obtención de la muestra debe ser fácil, cómoda y segura para conseguir la aceptación del usuario.
- Rendimiento: el nivel de precisión debe ser alto para obtener la confianza del usuario.

2.1.2 Modalidades y técnicas para el reconocimiento

Las modalidades biométricas se clasifican en dos grupos: físicas y de comportamiento.

Físicas: también son denominadas pasivas, son aquellas que para proceder a la identificación únicamente en necesario medir una característica del ser humano. Las más comunes son la huella dactilar, el iris, la geometría de la mano, el reconocimiento de retina o el reconocimiento facial entre otros. Algunos ejemplos se muestran en la figura 1 [2].

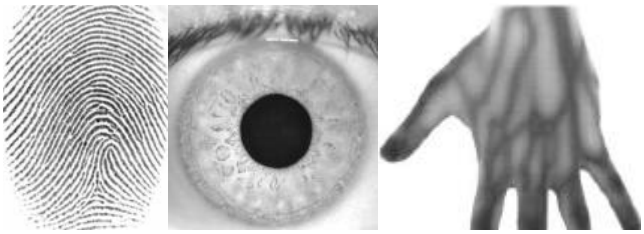

Figura 1. Ejemplos de modalidades físicas [4]

De comportamiento: también denominadas activas, son aquellas que se basan en la ejecución de una determinada actividad en presencia del sensor y es necesaria la participación activa del usuario. Las más comunes son la firma manuscrita o el reconocimiento del tecleo. En la figura 2 se muestran algunos ejemplos [2].

Figura 2. Ejemplos de modalidades de comportamiento [5] [6]

También se puede dar la combinación de ambas modalidades como ocurre en el caso de la voz.

El desarrollo de nuevas técnicas, para aumentar el número de modalidades para la identificación, está presente en la actualidad. Como es el caso de la geometría de la oreja o el olor corporal en el ámbito de la modalidad física y la forma de andar en la de comportamiento [2].

2.1.3 Sistema de reconocimiento biométrico

Los sistemas de reconocimiento biométrico son los encargados de obtener la muestra de la característica del individuo y procesar la información obtenida para proceder a la identificación.

Según la modalidad existen numerosos sistemas de reconocimiento diferentes pero en todos ellos existen subsistemas en común [2].

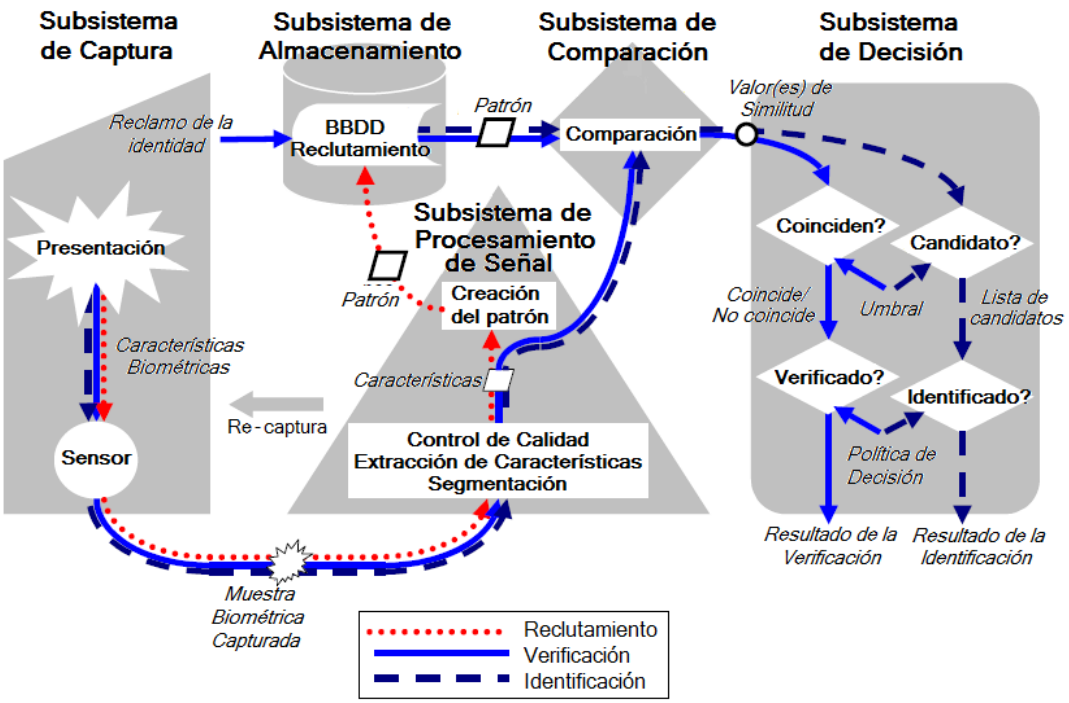

Figura 3. Subsistemas de un sistema de reconocimiento biométrico [7]

En la figura 3 se pueden distinguir los tres procesos diferenciados en cualquier sistema de reconocimiento biométrico: reclutamiento, verificación e identificación [8].

Reclutamiento: es el primer proceso dentro de un sistema de reconocimiento biométrico. Durante éste, se captura por primera vez la muestra del individuo a través del sensor correspondiente.
Esta muestra es procesada de manera que cuando se tenga la suficiente calidad se crea un patrón y se almacena en una base de datos.

Verificación: es el proceso de reconocimiento en que el usuario previamente se identifica y el sistema compara la muestra presentada con el patrón almacenado, lo cual dará un valor con el que se procederá a realizar la aceptación o rechazo del individuo.

Identificación: es el proceso de reconocimiento en el que el usuario presenta una muestra y el sistema realiza la comparación con todos los patrones existentes en la base de datos devolviendo una lista con los posibles candidatos.

La identificación puede ser de dos tipos:

- *Open-set:* cualquier usuario puede utilizar el sistema, aunque no haya sido reclutado anteriormente.
- *Closed-set:* solo los usuarios que han sido reclutados previamente podrán hacer uso del sistema [2].

2.1.4 Evaluación de los sistemas biométricos

Los sistemas biométricos deben pasar un análisis en el que se debe comprobar si cumplen con los requisitos, características y términos requeridos. Se busca detectar posibles fallos y determinar la aplicación más apropiada.

Existen distintos tipos de evaluaciones, según el análisis que se desee realizar. Entre los más comunes se encuentran [2] [8]:

Rendimiento: consiste en realizar el análisis de las características del sistema, como son la precisión, velocidad, fiabilidad, robustez, disponibilidad y el mantenimiento. Además de los factores que afectan al rendimiento como la interoperabilidad, escalabilidad, usabilidad y la influencia del entorno.

Con este análisis se obtiene la información más relevante del sistema para conocer su funcionamiento, tasas de error y tiempos de procesamiento.

Con las tasas de error se determina la precisión del sistema tanto en el proceso de reclutamiento como de reconocimiento, ya sea identificación o verificación.

Existen tres tipos de evaluación de rendimiento biométrico:

- **Tecnológica:** se encarga de analizar los algoritmos biométricos de la misma modalidad utilizando una base de datos genérica. Es un tipo de evaluación *offline*, es decir, el usuario no interactúa con el sistema en tiempo real. Es reproducible siempre y cuando los procedimientos y la base de datos sea la misma.
  Con este tipo de evaluación se permite analizar de forma separada los efectos de la interacción de los usuarios y la capacidad de los algoritmos empleados.

- **De escenario:** se realiza la evaluación en un entorno específico modelado según la aplicación real y las características de los usuarios que la utilizan.
  Puede ser *online*, es decir, el usuario interactúa con el sistema a tiempo real, o una combinación de *online* y *offline*. Al igual que la tecnológica es reproducible si se cumplen los mismos requisitos y condiciones.

- **Operacional:** la evaluación se realiza una vez que el sistema está instalado y funcionando en su entorno real siendo los usuarios los que finalmente usarán el sistema. Las evaluaciones se realizan *online* y no son reproducibles. La principal dificultad de esta evaluación es reconocer en el momento a la persona y determinar si es un genuino o impostor.

Seguridad: con este tipo de análisis se comprueba el cumplimiento de los requisitos de seguridad así como de la resistencia a potenciales ataques analizando su vulnerabilidad.

Para realizar este tipo de análisis es necesario conocer las tasas de error del sistema por lo que previamente es necesario realizar un análisis de rendimiento biométrico.

Aceptación del usuario: con este análisis se busca la opinión del usuario y su aceptación tras la experiencia adquirida con el uso del sistema.

También existen análisis de privacidad, seguridad del usuario o coste y beneficio entre otros.

Este proyecto se basa en la realización de una evaluación de rendimiento de un sistema de reconocimiento biométrico para la modalidad de huella dactilar. Como se ha comentado anteriormente, este tipo de análisis es de gran importancia, no solo por la obtención de las características del sistema, sino porque es necesaria para poder realizar un análisis de seguridad.

Cuanto mayor sea el rendimiento, más robusto y seguro será el sistema de reconocimiento con lo que se obtendrá mayor grado de aceptación.

Al tratarse de un análisis de rendimiento tecnológico se realizan pruebas sobre distintos algoritmos con el objetivo de conseguir un resultado aclaratorio sobre la fiabilidad y robustez del mismo así como su capacidad, tasas de error y tiempos de procesado tanto a la hora de realizar el reclutamiento como en la comparación ya sea identificación o verificación.

Las pruebas deben realizarse sobre la misma base de datos previamente obtenida y normalizada.

Al no modificar la base de datos y ser *offline*, es decir, el usuario no tiene que estar presente, la evaluación es repetible tantas veces como sea necesario siempre que se siga el mismo proceso en el análisis.

La biometría se basa en probabilidades, por lo que la cantidad de muestras de usuarios que formen la base de datos debe ser la más significativa posible para poder tener mayor fiabilidad en los resultados obtenidos.

La evaluación debe realizarse de forma objetiva y bajo unos estándares para evitar todo tipo de fraudes y falsos datos que puedan dar lugar a engaño.

Para ello se crearon metodologías bajo distintos estándares internacionales, en continua renovación, para efectuar de forma correcta una evaluación de manera que se permita la reproductividad de la misma.

Estas metodologías determinan cómo planificar, efectuar y documentar una evaluación [2].

2.1.5 Medidas de rendimiento

Como ya se ha comentado anteriormente, las medidas de rendimiento se basan en las tasas de error y de *throughput* [2] [3]. Las cuales determinan la precisión del sistema tanto en el reclutamiento como en el reconocimiento. A continuación, se detallan las diferentes tasas más comunes para los sistemas de reconocimiento biométrico.

Tasas de error:

Se pretende cuantificar la precisión midiendo el número de errores cometidos durante los procesos de reconocimiento. Existen distintos tipos según el proceso.

Fallos durante el proceso de adquisición y procesamiento de señal:

- **FTE**: cuando el fallo ocurre durante el reclutamiento. Define el número de usuarios que no son aceptados por el sistema a la hora de realizar el reclutamiento.
- **FTA**: cuando el fallo se produce durante el reconocimiento. Contabiliza el número de intentos en los que el sistema ha fallado a pesar de contar con una muestro de buena calidad.

Fallos durante el proceso de comparación y decisión:

- **FNMR**: número de intentos de reconocimiento para los cuales el sistema ha dado error a pesar de tratarse del usuario correcto.
- **FMR**: número de intentos de reconocimiento para los cuales el sistema no ha dado error a pesar de tratarse de un usuario incorrecto.

Fallos durante el proceso de verificación:

- **FRR**: número de veces que el usuario es rechazado a pesar de ser el genuino.
- **FAR**: número de veces que el usuario es aceptado a pesar de ser un impostor.
- **EER**: punto en el que el FNMR o FRR es igual al FMR o FAR.

Fallos durante el proceso de identificación:

- **FNIR**: número de veces que, para los usuarios reclutados, no aparece su identificación en la lista de candidatos proporcionada por el sistema.
- **FPIR**: número de veces que, para los usuarios no reclutados, la lista propuesta por el sistema no está vacía.
- **Tasa de identificación**: número de veces que el usuario correcto sale en la lista propuesta por el sistema.

Tasas de *throughput*:

Este tipo de tasas tiene como fin cuantificar el tiempo necesario para realizar cada proceso, es decir, mide el tiempo de reclutamiento y el tiempo de reconocimiento, tanto el de captura como el de comparación. El cálculo se lleva a cabo teniendo en cuenta el conjunto de usuarios que han participado durante la evaluación [8].

Típicamente para realizar un análisis de rendimiento se emplean gráficas representativas de las medidas del mismo. Las gráficas más comunes son: gráfica FMR frente FNMR, curva DET y curva ROC.

Gráfica FMR frente FNMR

Este gráfico representa la distribución que siguen dos posibles fallos durante el proceso de comparación y decisión: el FMR y FNMR.

El eje de abscisas corresponde con el valor umbral y el eje de ordenadas con la probabilidad de error.

El punto característico de este tipo de gráficos es en el que la curva FNMR se cruza con la FMR, denominado EER (*equal error rate*).

Si se realiza un desplazamiento a la derecha a partir del EER la probabilidad de obtener un error a pesar de tratarse de un usuario correcto aumenta mientras que la probabilidad de que haya una falsa aceptación disminuye, es decir, la probabilidad de error de un FNMR aumenta mientras que la de FMR disminuye.

Por el contrario, si el desplazamiento se realiza hacia la izquierda del EER la probabilidad de error de un FMR aumenta mientras que la de un FNMR disminuye.

Este gráfico es de vital importancia dado que con la obtención del EER se establecen los parámetros que determinan el grado de aceptación ante posibles fraudes al sistema de reconocimiento, realizando el compromiso de nivel de seguridad del sistema [30].

La figura 4 muestra un gráfica típica de FMR frente a FNMR.

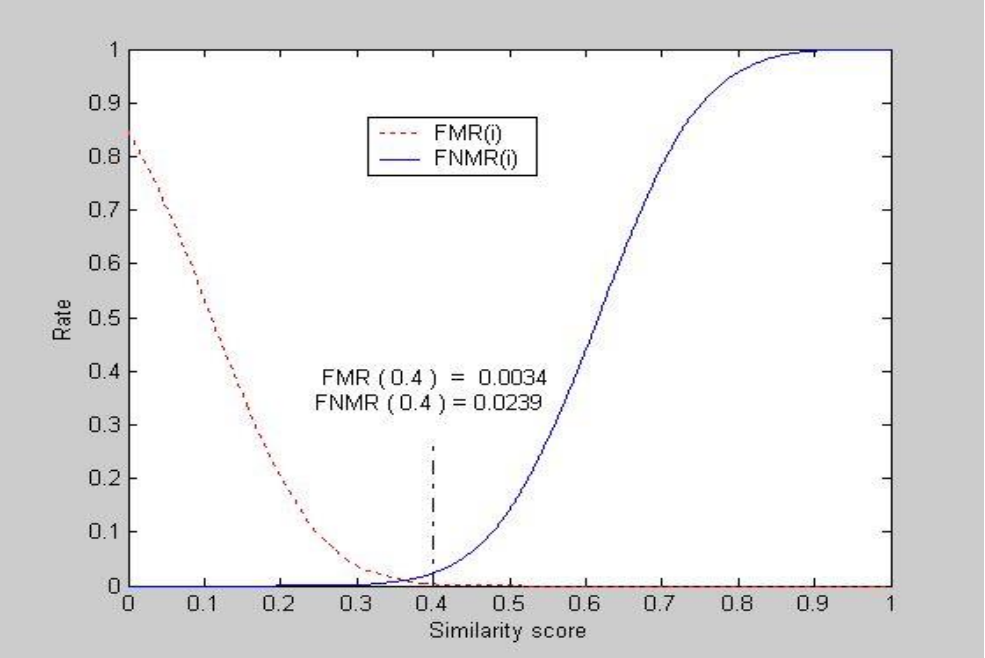

Figura 4. Ejemplo gráfica FMR vs FMRN [30]

Curva de Compensación del Error de Detección. DET

Esta curva representa la desviación estándar de las probabilidades de error de falso rechazo frente a las de falsa aceptación, es decir, FNMR frente a FMR.

La linealidad obtenida es resultado de asumir que la densidad de probabilidad es normal y que la pendiente es unitaria debido a que las varianzas en la distribución son iguales.

Cuanto más se acerque la curva a la esquina inferior izquierda menor será la probabilidad de fallo y por lo tanto mejor serán los resultados.

Una curva DET característica se muestra en la figura 5 [31].

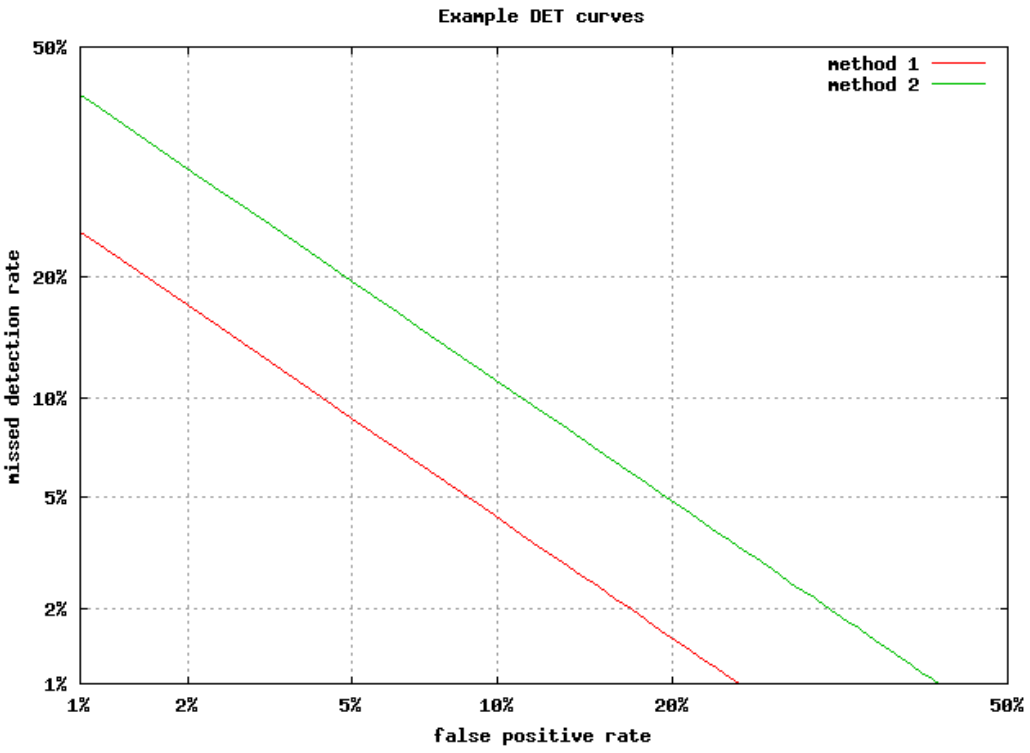

Figura 5. Ejemplo curva DET [31]

Curva Característica de Operación del Receptor. ROC

A diferencia de la curva DET, la curva ROC representa las probabilidades de error de falsa aceptación frente a las de falso rechazo, es decir, FMR frente a (1-FNMR).

Esta curva permite ajustar el punto de operación de un detector o estable el mejor punto para la toma de decisiones.

El espacio ROC representa la los intercambios entre verdadera y falsa aceptación.

El valor del EER se puede obtener trazando la diagonal entre la esquina superior izquierda y la inferior derecha, dónde se corte la diagonal con la curva corresponde al punto del valor del EER.

Cuanto más se acerque la curva a la esquina superior izquierda, menor será la probabilidad de fallo y por lo tanto mejor será el resultado.

Una curva ROC característica se muestra en la figura 6 [32].

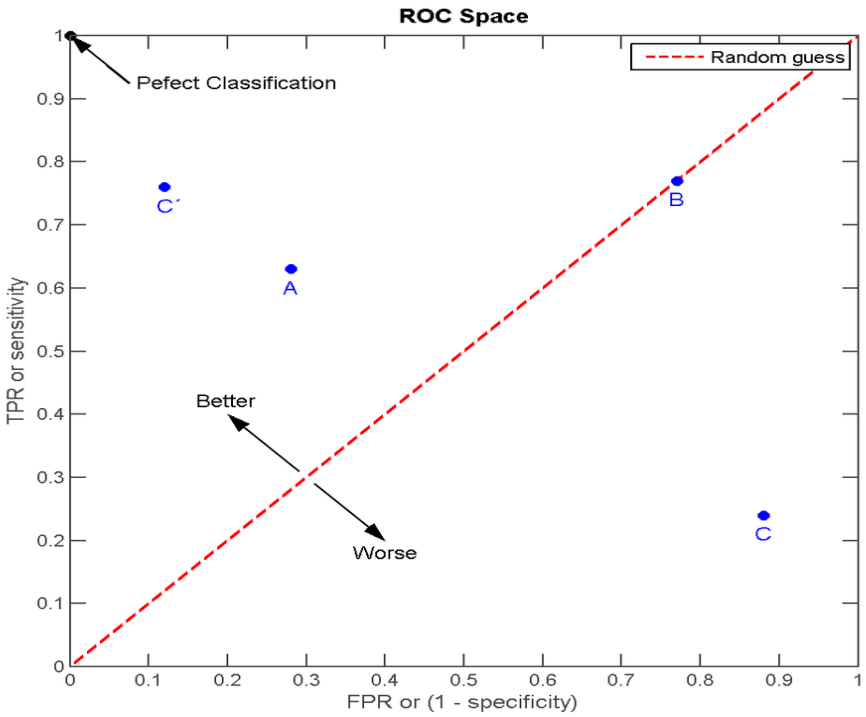

Figura 6. Ejemplo curva ROC [32]

2.2 Huella dactilar

Las huellas dactilares son identificadores genéticos únicos de cada ser humano. No existen dos individuos con las mismas huellas, ni si quiera en el caso de gemelos.

Las huellas dactilares se forman en el embrión aproximadamente a partir de las diez semanas de gestación, y las últimas investigaciones, realizadas por científicos de la Universidad de Arizona, apuntan a que la formación se debe a las tensiones producidas por las distintas capas de la piel. Concretamente al rápido crecimiento de la capa basal, situada entre la dermis externa e interna, lo que produce las tensiones que dan lugar a las "arrugas" que forman las huellas.

La investigación acerca de las huellas dactilares lleva produciéndose desde hace siglos. En 1686 Marcello Malpighi realizó un tratado sobre las capas de la piel, dónde señaló las diferencias en los patrones de las huellas [3].

Sir Francis Galton publicó en 1892 el libro FingerPrints que recogía las tres leyes fundamentales de la dactiloscopia: perennidad, inmutabilidad y diversidad infinita. Además estableció un método de clasificación e identificó las minucias: rasgos específicos de una huella dactilar [3].

2.2.1 Partes de una huella dactilar

Marcello Malpighi determinó las diferencias encontradas en las "arrugas" de los patrones de huellas dactilares, definiendo las crestas y valles o surcos [3].

Se entienden por crestas las líneas que se encuentran en relieve respecto de la yema del dedo, mientras que los valles hacen referencia a las hendiduras encontradas.

Cuando se realiza una impresión de la huella dactilar las líneas negras corresponden a las crestas mientras que las líneas blancas a los valles, como puede observarse en la figura 7:

(a) (b)

Figura 7. (a) Ejemplo huella dactilar [10]. (b) Ejemplo impresión de huella dactilar [11]

Existen varios tipos de huellas, pudiendo ser clasificadas según las formas que siguen las crestas y valles. Esta clasificación se encuentra en la figura 8 [12].

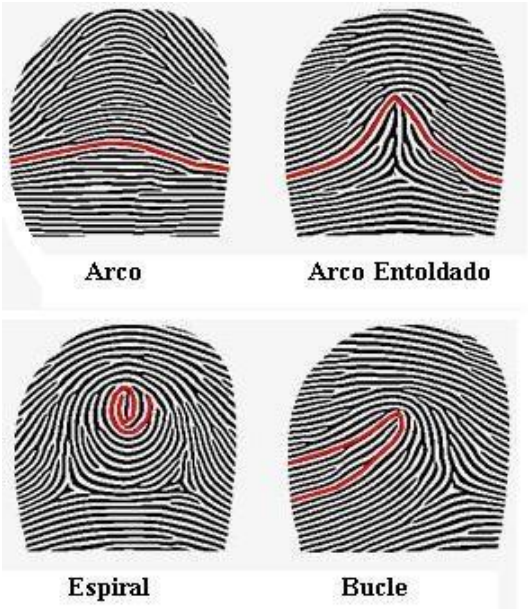

Figura 8. Clasificación de los tipos de patrones de huella dactilar [13]

Al igual que se realiza una clasificación de los distintos patrones encontrados en las huellas, también es posible clasificar los puntos característicos que los forman, es decir, la clasificación de los distintos tipos de minucias. Esta clasificación se puede encontrar en la figura 9 [12] [33].

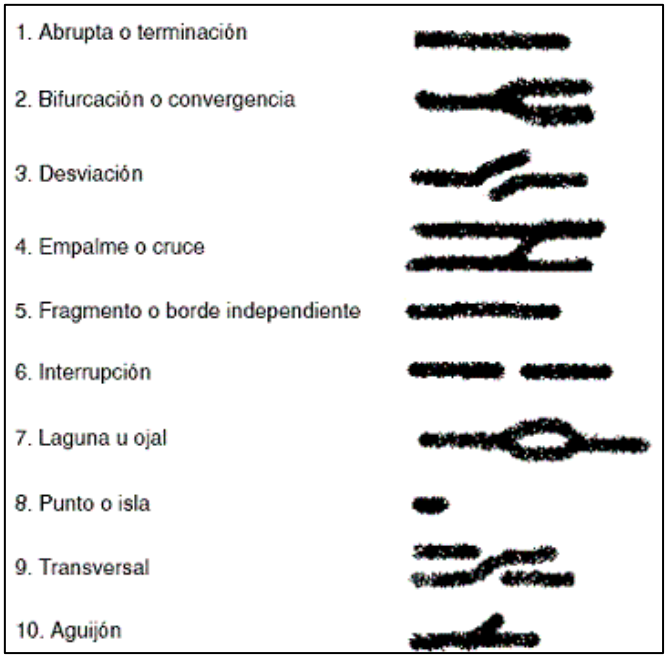

Figura 9. Clasificación de los tipos de minucias de una huella dactilar [14]

2.3 Sistemas de reconocimiento de huella dactilar

Los sistemas de reconocimiento biométrico consisten en el reconocimiento automático de un individuo tras presentar un rasgo característico.

En la modalidad de huella, el rasgo característico presentado al sistema es la propia huella dactilar mediante sensores específicos [34] [35].

Los sistemas de reconocimiento se pueden basar en técnicas de comparación basadas en minucias o en correlación.

La técnica basada en minucias consiste en la extracción de las características específicas de la huellas, generando un mapa en el que se localiza la posición y la orientación precisa de cada minucia. Al tratarse de una aproximación, este método puede presentar algunos fallos como es la obtención de falsas minucias, sobre todo cuando la calidad de la imagen es baja [8] [16].

Por otro lado, la técnica basada en la correlación no realiza una extracción de las características específicas sino que se almacena la muestra en su conjunto [16]. De este modo se pretende solventar algunos de los fallos de los métodos basados en minucias, pero aun así tiene algunos propios, dado que requiere una localización precisa que se puede ver afectada por la rotación o traslación de la muestra durante la captura.

2.3.1 Algoritmos para el reconocimiento de huella dactilar

La Real Academia Española recoge como definición de algoritmo al conjunto ordenado y finito de operaciones que permiten hallar la solución de un problema [19].

Los algoritmos implementados en sistemas de reconocimiento basados en minucias buscan la transformación matemática de la posición y orientación de estos puntos característicos para almacenarlos y poder así realizar la comparación, estimando el grado de similitud.

En el caso de los algoritmos implementados en sistemas de reconocimiento basados en correlación se busca la obtención del patrón completo de la muestra. La comparación se realiza calculando la correlación que existe entre dos imágenes, es decir, se superpone una imagen a la otra y se comprueba si coinciden.

Esta técnica da lugar a errores en el caso de que las imágenes estén desplazadas entre sí o una rotación en el momento de la adquisición. También dependen de la elasticidad de la piel que impida el correcto alineamiento de las imágenes [16] [20].

2.3.2 Sensores de huella dactilar

La obtención de la muestra de cada huella se realiza a través de lectores biométricos o sensores. Existen varios tipos de sensores y su clasificación se realiza según la tecnología empleada para la adquisición de la muestra: capacitivos, ópticos, térmicos o de presión [17].

- Los **sensores ópticos** se basan en dispositivos CCD (Charged Coupled Device) junto con un *array* de fotodiodos además de contar con una fuente de iluminación propia, típicamente con un *array* de LEDs.

  La imagen se forma a través de los contrastes generados por los cambios de luz producidos por las crestas y los valles al colocar el dedo sobre el sensor, estos cambios de luz son recogidos por los fotodiodos, que determinan el color del píxel.

  Las crestas dan píxeles negros y los valles blancos. La resolución de la huella digital obtenida depende del número de fotodiodos del que esté formado y la calidad de la imagen obtenida viene influida por el tipo de piel del individuo así como de la sudoración presente y la suciedad.

  En la figura 10 se muestra un esquema del funcionamiento de los sensores ópticos.

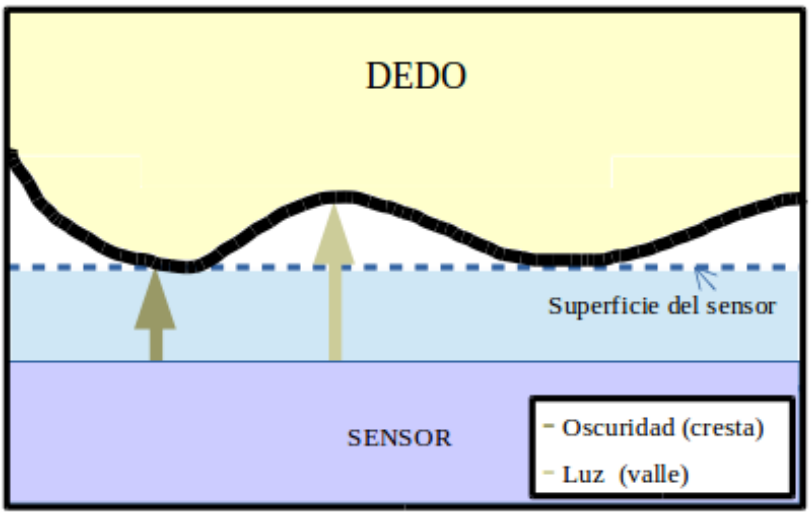

Figura 10. Esquema de funcionamiento de un sensor óptico de huella dactilar

- Los **sensores de presión o mecánicos** están formados por una superficie compuesta de miles sensores de presión diminutos que reaccionan ante la fuerza ejercida por el dedo.
- Los **sensores capacitivos** se basan en el cambio de corriente eléctrica. Para ello la superficie del sensor cuenta con un *array* de condensadores planos. Al colocar el dedo sobre el sensor, éste actúa como otra placa del condensador mientras que las distintas profundidades entre las crestas y los valles modifican la cantidad de dieléctrico generando capacitancias distintas, lo que da lugar a obtener la huella digital.

La tensión eléctrica ante una cresta es mayor que ante un valle.

La calidad de la imagen puede ser mejorada realizando ajustes en algunos parámetros eléctricos del sensor, muy útil cuando la muestra presentada pertenece a un usuario con piel muy húmeda o seca.

Al no utilizar un dispositivo CCD, los sensores capacitivos son más compactos que los ópticos, pero deben ser limpiados continuamente para evitar que la suciedad empeore la calidad de la imagen.

Se muestra un esquema descriptivo en la figura 11 [17] [37].

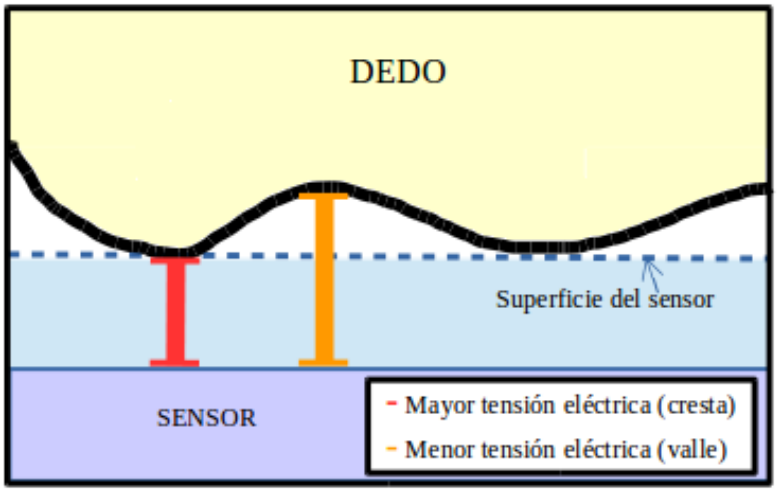

Figura 11. Esquema de funcionamiento de un sensor capacitivo de huella dactilar

- Los **sensores térmicos** se basan en la captación del calor que transmite el dedo del individuo por medio de materiales termoeléctricos. Las crestas generan más calor que los valles por esta razón se consigue obtener el patrón de la huella dactilar presentada.

  Presentan la ventaja de no ser sensibles a descargas electrostáticas.

  En la figura 12 se muestra un esquema de un sensor térmico [18].

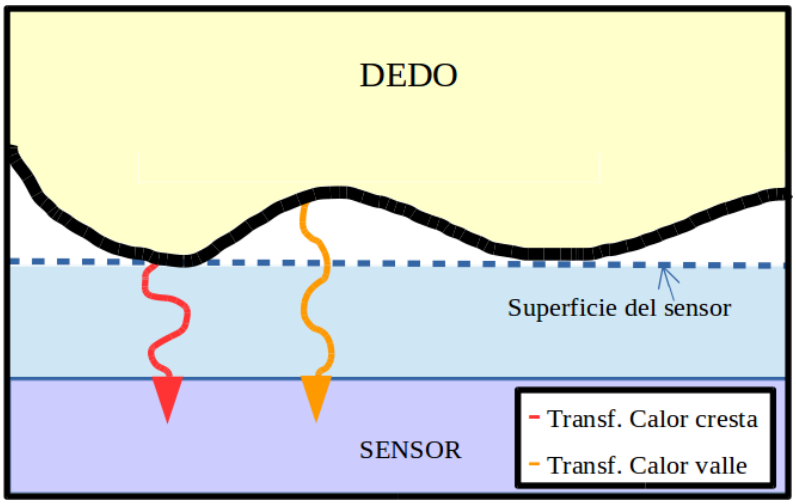

Figura 12. Esquema de funcionamiento de un sensor térmico de huella dactilar

Los sensores utilizados, para generar la base de datos de este estudio, se presentan a continuación. Como ya se ha comentado anteriormente se tratan de uno de tipo térmico y los otros dos de tipo capacitivo.

Sensor NB-3010-U (NXT)

Este sensor se basa en la tecnología térmica para obtener la captura de la huella.

Al presentar la huella sobre el sensor éste recoge la temperatura proporcionada por la huella creando la imagen digital de la misma.

Las crestas de las huellas transfieren más calor que los valles por lo tanto los píxeles negros corresponden a las crestas mientras que los blancos a los valles.

En la figura 13 se muestra una imagen del sensor, y en la tabla 1 las principales especificaciones técnicas que presenta [26].

Figura 13. Sensor de huella NB-3010-U. NXT [27]

Tabla 1. Especificaciones sensor NXT

NXT: NB-3010-U	
Tecnología del sensor	NEXT Active ThermalTM sensing, patentada por NEXT Biometrics
Área activa del sensor (mm)	11.9 x 16.9
Resolución (ppi)	385
Niveles escala de grises	256
Tamaño imagen de la huella (píxeles)	180 x 256

Sensor FPC1011F3 (FPC)

Este sensor se basa en la tecnología capacitiva para obtener la captura de la huella.

Al presentar la huella sobre el sensor, éste mide las diferentes capacitancias generadas al existir diferente cantidad de dieléctrico entre los valles y las crestas.

Las crestas de las huellas corresponden a los píxeles negros dado que tienen menor cantidad de dieléctrico que los valles, por los que estos últimos son representados con píxeles blancos.

En la figura 14 se muestra una imagen del sensor, y en la tabla 2 las principales especificaciones técnicas que presenta [26].

Figura 14. Sensor de huella FPC1011F3. FPC [28]

Tabla 2. Especificaciones sensor FPC

FPC: FPC1011F3	
Área activa del sensor (mm)	10.64 x 14.0
Resolución (dpi)	363
Niveles escala de grises	256
Tamaño imagen de la huella (píxeles)	152 x 200

Sensor UPEK EikonTouch 510 (UPK)

Este sensor se basa en la tecnología capacitiva para obtener la captura de la huella.

Al presentar la huella sobre el sensor, éste mide las diferentes capacitancias generadas al existir diferente cantidad de dieléctrico entre los valles y las crestas.

Las crestas de las huellas corresponden a los píxeles negros dado que tienen menor cantidad de dieléctrico que los valles, por los que estos últimos son representados con píxeles blancos.

Figura 15. Sensor UPEK EikonTouch 510- UPK [29]

En la figura 15 se muestra una imagen del sensor, y en la tabla 3 las principales especificaciones técnicas que presenta [26].

Tabla 3. Especificaciones sensor UPK

UPK: UPEK EikonTouch 510	
Área activa del sensor (mm)	12.8 x 18.0
Resolución (dpi)	508
Niveles escala de grises	256
Tamaño imagen de la huella (píxeles)	192 x 270

CAPÍTULO 3. DISEÑO DEL PROYECTO

El tercer capítulo del documento está destinado a la explicación del diseño llevado a cabo con el fin de cumplir con los objetivos marcados para este estudio.

Por lo que en los siguientes apartados se encuentran los algoritmos a analizar junto con las herramientas empleadas para ello: la base de datos, las aplicaciones diseñadas y los softwares para el uso de los distintos algoritmos.

3.1 Diseño del estudio de rendimiento tecnológico de un sistema biométrico de huella dactilar

El objetivo principal de este estudio es realizar un análisis de rendimiento de dos algoritmos, para la modalidad de huella dactilar, por lo que es necesario hacer una evaluación de rendimiento tecnológico.

En el estudio se debía conseguir un valor de comparación al procesar distintas imágenes tomadas con sensores diferentes bajo los dos algoritmos utilizados.

Para cumplir con este objetivo se hizo un primer diseño en el que se pretendía realizar una aplicación capaz de procesar una imagen seleccionada, independientemente del sensor usado para la captura, y bajo la elección de uno de los dos algoritmos a analizar, y compararla con otra devolviendo el resultado.

Estos datos resultantes de la comparación debían ser guardados en un fichero que permitiera su posterior uso para la obtención de un resultado gráfico con el que se permitiera obtener conclusiones precisas acerca del rendimiento de los algoritmos empleados.

Por lo tanto el diseño del estudio se planteó de manera que constara de dos partes:

Una primera en la que se buscaba la obtención de los resultados de la comparación entre dos muestras usando dos softwares de análisis de algoritmos distintos: NIST Biometric Image Software (NBIS) y MCC Software Development Kit (MCC SDK), con las muestras de una base de datos obtenidas por tres sensores distintos: uno térmico, NB-3010-U (NXT) y dos capacitivos: FPC1011F3 (FPC) y UPEK EikonTouch 510 (UPK).

Por lo tanto esta aplicación, que realiza las comparaciones, debía ser ejecutada tres veces para obtener los resultados de rendimiento al trabajar con el algoritmo NBIS y las muestras obtenidas con los sensores NXT, FPC y NXT. Y del mismo modo también se tenía que ejecutar otras tres veces para obtener los resultados al trabajar con el algoritmo MCC y las muestras de los tres sensores.

Durante la segunda parte se debía obtener las medidas de rendimiento gráficas de los datos generados en la primera, para ello se implementó una aplicación capaz de gestionar y analizar dichos datos.

3.2 Algoritmos a analizar

Se ha realizado una evaluación de rendimiento tecnológico para analizar dos algoritmos de sistemas de reconocimiento de huella dactilar. Uno de los cuales es convencional, es decir, la extracción de las características de la huella las realiza mediante aproximaciones a las minucias vecinas, mientras que el otro se basa en códigos cilíndricos el cual se asienta en la representación de estructuras locales.

A continuación se presentan los softwares empleados para realizar el análisis junto con una explicación de los distintos algoritmos.

NIST Biometric Image Software (NBIS)

Este software desarrollado por el National Institute of Standards and Technology (NIST) para el Federal Bureau of Investigation (FBI) se organiza en dos categorías: *the non-export controlled* y *the export controlled*. [21]

Este algoritmo fue implementado bajo el estándar ANSI/NIST-ITL 1-2007, el cual define un formato de archivo común para el intercambio electrónico de huellas digitales y datos relacionados con las mismas.

Del paquete de *non-export controlled* se ha utilizado el sistema de detección de minucias: MINDTCT, mientras que del *export controlled* se ha utilizado el sistema de comparación de huellas dactilares: BOZORTH3.

Ambos sistemas son compatibles entre sí, y su uso está relacionado dado que con los resultados obtenidos del MINDTCT se obtienen los resultados de comparación en el BOZORTH3.

MINDTCT. Sistema de detección de minucias

Dos huellas pueden ser comparadas a través de las minucias que presentan permitiendo determinar si se trata del mismo individuo en ambos casos. Típicamente hay unas cien minucias por huella.

Este sistema detecta las minucias existentes en la huella digital almacenando las coordenadas de localización y orientación de cada una de ellas. La distancia de coordenadas viene definida por el estándar ANSI/NIST-ITL 1-2007 que especifica unidades de distancia de 0,01 mm y la orientación viene representada en grados.

El algoritmo interno del MINDTCT consta de ocho pasos.

1. Entrada de archivo de huella digital: las imágenes cargadas deben de haber sido escaneadas bajo un formato de 19,69 ppmm y a una escala de grises de 256 niveles.

2. Generar mapa de imagen: la calidad de la imagen puede variar por lo que se genera un mapa de imagen con el que se determina las zonas de baja calidad o las que pueden dar lugar a fallo.

3. Imagen binarizada: el algoritmo de detección de minucias está diseñado para trabajar en niveles binarios. Por lo que es necesario transformar la imagen de entrada en escala de grises a únicamente dos píxeles de color: negro o blanco.

4. Detectar minucias: en este paso se analiza la imagen binaria obtenida anteriormente con el fin de encontrar las características específicas. Para ello se analiza la imagen por patrones en los que según el color del conjunto de píxeles se determina el tipo de característica que presenta la muestra. En la figura 16 se muestran los patrones usados para determinar el tipo de minucia.

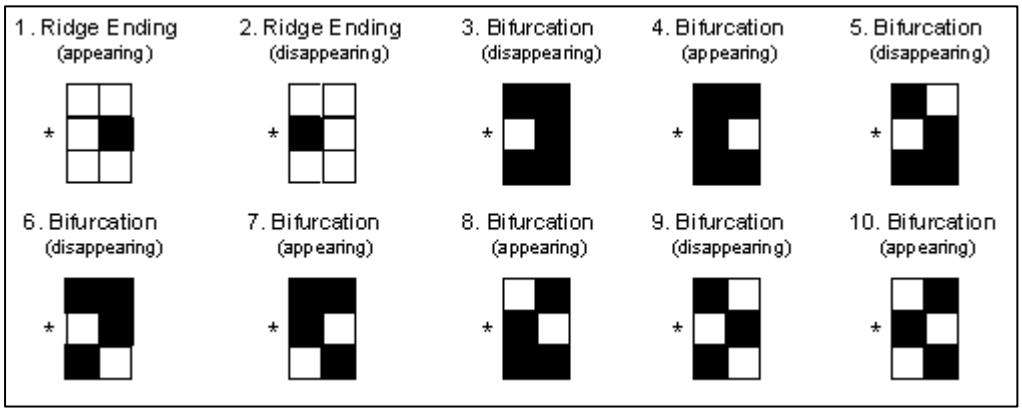

Figura 16. Patrones de píxel usados para detectar minucias [22]

5. Eliminar falsas minucias: utilizar patrones para detectar posibles minucias puede acarrear la obtención de falsas minucias por lo que es necesario eliminarlas. Este algoritmo cuenta con su propio método para eliminar las falsas minucias da igual el tipo que sean o si se han producido por una baja calidad.

6. Contar crestas vecinas: los comparadores de minucias a veces usan información adicional a los puntos característicos. Por lo tanto, además de analizar la posición y orientación de la minucia se analiza la situación de la minucia vecina.

Un atributo muy empleado es el número de crestas intervenidas, también conocido como '*ridge crossings',* entre una minucia y su vecina.

7. Evaluar calidad minucias: la evaluación de la calidad asociada a las minucias extraídas es de gran importancia para poder determinar si los resultados obtenidos se tratan de puntos característicos o por el contrario de falsas minucias. Por lo tanto a las falsas minucias se les debe asignar una baja calidad mientras que a la calidad de las verdaderas debe ser alta.

8. Archivos de salida de minucias: una vez completado el MINDTCT se obtiene un fichero de salida en el que se encuentra las minucias encontradas como se puede observar en la figura 17:

Figura 17. Ejemplo minucias obtenidas [23]

BOZORTH3. Sistema de comparación de huellas

Este sistema compara las minucias de dos muestras procesadas previamente por el sistema MINDTCT obteniendo un valor de comparación comprendido entre 0 y 300.

Cuanto mayor sea el resultado de comparación mayor será la probabilidad de que las muestras comparadas sean del mismo dedo de un individuo.

MCC Software Development Kit (SDK) 2.0

El algoritmo MCC se basa en la representación de estructuras locales. Este tipo de método nace para solventar los problemas de los algoritmos convencionales de huella dactilar provocados por la no linealidad de la huella.

Dicha representación se realiza de forma que cada minucia cuenta con una estructura local que codifica las relaciones espaciales y direccionales entre la minucia y sus vecinas, fijando un radio de curvatura. Es conveniente realizar una representación cilíndrica cuya base corresponde a la información espacial y la altura a la información direccional.

La figura 18 muestra un esquema representativo del funcionamiento del MCC.

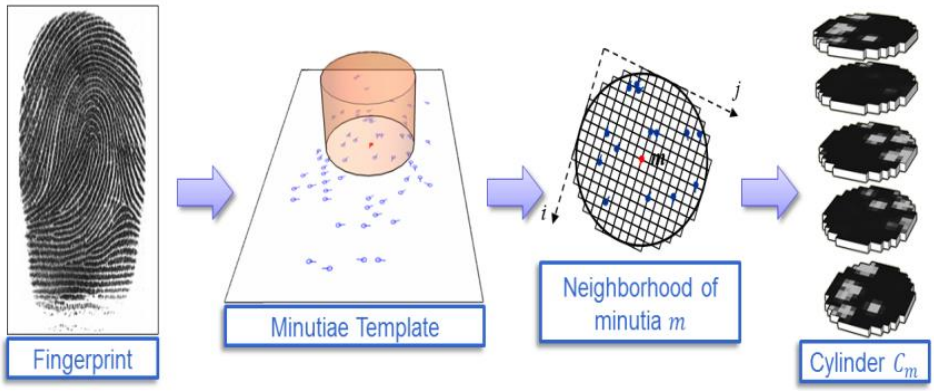

Figura 18. Esquema funcionamiento algoritmo MCC [25]

El uso de aproximaciones por radio fijo permite obtener mejores tolerancias de minucias perdidas o falsas que en el caso de los métodos basados en aproximaciones de vecinos cercanos.

El MCC SDK es una librería DLL .Net válida para aplicaciones de verificación de huellas dactilares usando los algoritmos MCC [24].

Este software da como resultado de la comparación valores entre 0 y 1, con una resolución de dieciséis decimales.

Cuando el valor está cercano a cero significa que se trata de un impostor mientras que si está cercano a uno se trata de un genuino.

3.3 Descripción de la base de datos empleada

Como ya se introdujo en el Capítulo 1, la realización de este estudio se ha llevado a cabo empleando una base de datos capturada durante las prácticas de empresa en el GUTI.

Las prácticas consistían en la captura de una base de datos para tres sensores biométricos de huella dactilar: NXT, FPC y UPK.

Durante la evaluación se registraron un total de 589 usuarios obteniendo una base de datos de 188216 muestras.

Las muestras de cada usuario se encuentran almacenadas en carpetas, nombradas con el identificador del mismo dentro de la base de datos.

Existen dos tipos de muestras para cada usuario: las muestras de reclutamiento (EN) y las muestras de verificación (V):

- **Muestras de reclutamiento:** estas muestras se obtuvieron en el reclutamiento del usuario. Se pueden encontrar un máximo de 36 muestras de reclutamiento por usuario.
- **Muestras de verificación:** estas muestras corresponden a las obtenidas durante el procedimiento de verificación.
  La verificación constaba de dos visitas por lo que las muestras se nombran con V1 o V2, según correspondiera a la primera o segunda visita respectivamente. El número máximo de muestras de verificación por usuario es de 108.

La base de datos utilizada en este estudio constaba de un total de 15037 muestras, obtenidas de los dedos pulgar, índice y corazón de ambas manos de cincuenta usuarios.

3.4 Descripción de los requisitos de la aplicación de comparación

La primera parte del proyecto se basa en la implementación de una aplicación que realizara el procesamiento de la base de datos utilizando ambos algoritmos.

La aplicación a realizar debía ser capaz de escoger el algoritmo, y las muestras del sensor deseadas para la comparación. Es decir debía poder escogerse NBIS o MCC y NXT, FPC o UPK.

El programa almacena en la variable 'muestra 1' una imagen de reclutamiento correspondiente a cada dedo del usuario y en la variable 'muestra 2' una imagen de cada verificación almacenada en la base de datos para ese usuario.

Una vez obtenidos los vectores de características de ambas muestras, se realiza la comparación de las mismas almacenando el resultado en dos ficheros según el siguiente criterio:

Si 'muestra 1' y 'muestra 2' corresponden al mismo usuario y al mismo dedo el resultado se almacena en el fichero de genuinos: fGENUINOS.txt, si por el contrario la 'muestra 1' y la 'muestra 2' corresponden a usuarios distintos el valor obtenido en la comparación se almacena en el fichero de impostores: fIMPOSTORES.txt.

En la figura 19 se muestra un diagrama de flujo el cual representa el funcionamiento de la aplicación a realizada, donde:

- **ID** es el identificador de la muestra
- **M1** corresponde a la muestra 1
- **M2** corresponde a la muestra 2
- **EN** es la captura del reclutamiento
- **V** es la captura de la verificación
- **MÁX** es el valor máximo de muestras
- **x** es el identificador del dedo de la muestra de reclutamiento
- **y** es el identificador del número de muestra de verificación

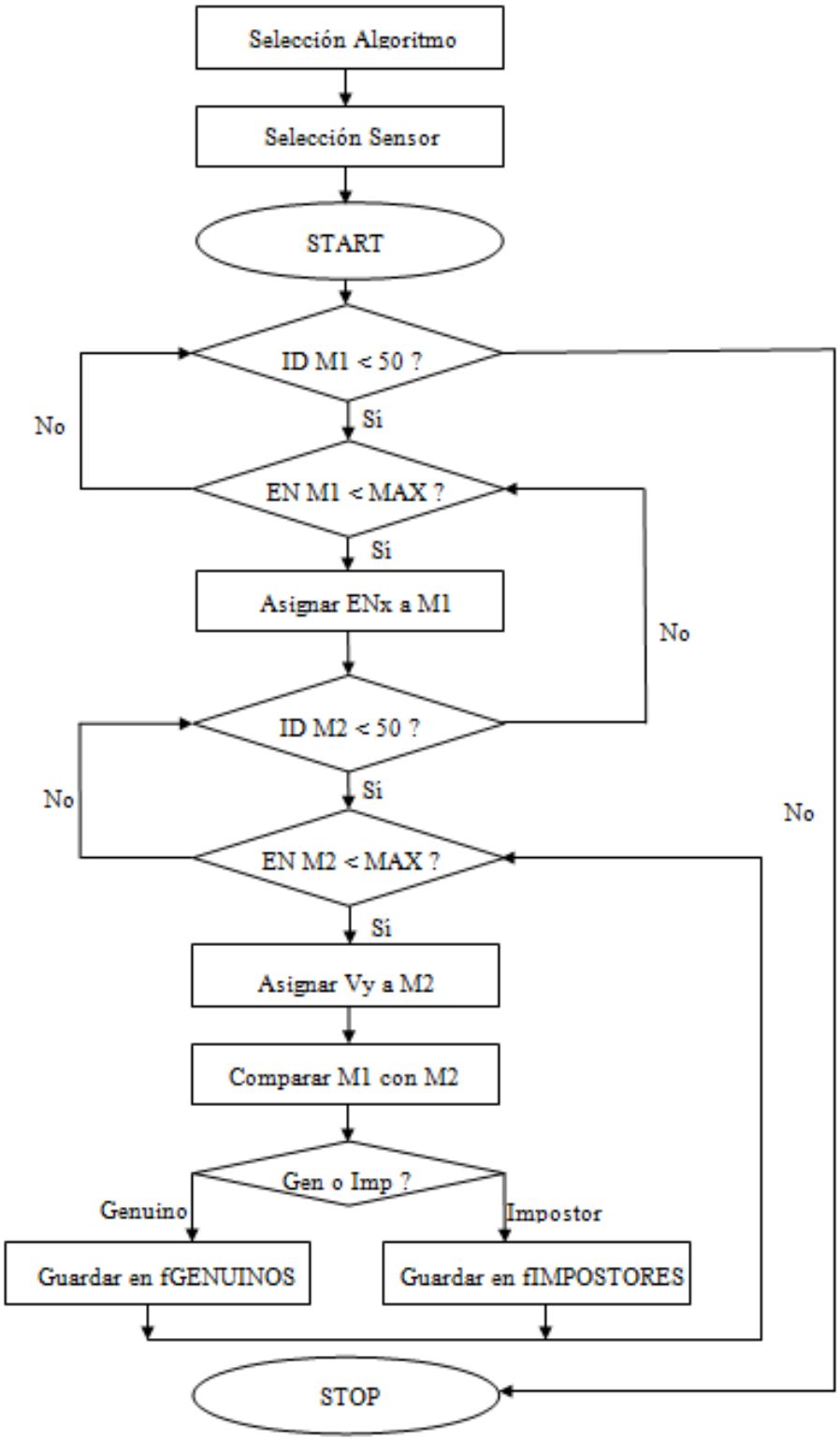

Figura 19. Flujograma de la aplicación de comparación

3.5 Descripción de los requisitos de la aplicación para la obtención de los resultados gráficos

La segunda parte del proyecto se basa en la implementación de una aplicación para obtener las medidas de rendimiento gráficas, a partir de los datos de comparación obtenidos por la aplicación anterior.

Esta aplicación debía generar las gráficas de medida de rendimiento: gráfica FMR frente FNMR, curva DET y curva ROC, a partir de los ficheros generados en la aplicación de comparación, correspondientes al procesado de las muestras de los tres sensores con los dos algoritmos posibles, es decir, un total de doce ficheros: seis de impostores y seis de genuinos correspondientes al procesado de NBIS-NXT, NBIS-FPC, NBIS-UPK, MCC-NXT, MCC-FPC y MCC-UPK.

CAPÍTULO 4. DESARROLLO DEL PROYECTO

Este proyecto consta de dos partes: una primera donde se realiza la comparación entre dos huellas, almacenando el resultado en un fichero. Y una segunda parte en la que se analizan dichos resultados de forma gráfica. Para realizar ambas partes se han implementado dos aplicaciones.

En este capítulo se describe el desarrollo seguido hasta la obtención de dichas aplicaciones.

4.1 Desarrollo de la aplicación de comparación

La aplicación para la comparación de muestras de huellas dactilares se desarrolla bajo el entorno Microsoft Visual Studio 2013.

La decisión del uso de este entorno se tomó dado que éste permite trabajar con múltiples lenguajes de programación como son C++, C# o .NET entre otros, aunque el lenguaje utilizado para este estudio ha sido C#.

Además el entorno Visual Studio permite realizar tanto aplicaciones de consola como de escritorio (Windows Presentation Foundation: WPF).

El procedimiento hasta obtener la aplicación final constó de varias fases o pruebas.

Fase 1. Aplicación de consola para algoritmo NBIS con base de datos reducida

En esta primera fase se realizó una aplicación de consola que realizará la comparación de las muestras bajo el algoritmo NBIS. La base de datos se redujo a tres usuarios con un total de 179 muestras.

La aplicación mostraba los tres usuarios disponibles con los que realizar la comparación, una vez escogido el usuario mostraba las muestras disponibles para la variable 'muestra 1' y posteriormente para la 'muestra 2'. Una vez asignadas ambas muestras comenzaba la comparación imprimiendo por pantalla el número de minucias obtenidas de cada muestra y el resultado de la comparación, además de ser almacenado este último en el fichero correspondiente.

En la figura 20 se muestra la aplicación de consola desarrollada.

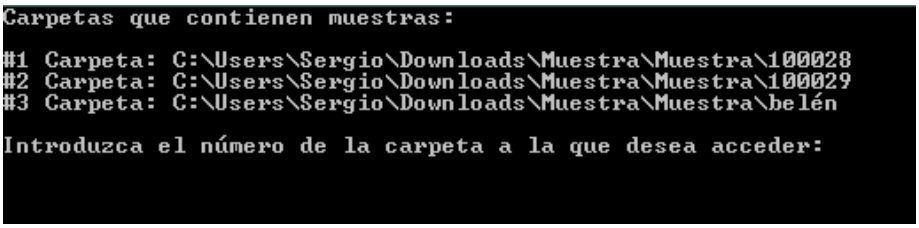

Figura 20. Aplicación de consola

Fase 2. Aplicación de consola para algoritmo NBIS

Tras finalizar la fase 1 con éxito, se modificó el código implementado para permitir utilizar la base de datos al completo, con un total de 15037 muestras.

Fase 3. Aplicación de consola para algoritmo MCC con base de datos reducida

Del mismo modo que para el algoritmo NBIS, se procedió a realizar una aplicación de consola en la que se realizara la comparación bajo el algoritmo MCC con la reducción de la base de datos a tres usuarios únicamente.

Fase 4. Aplicación de consola para algoritmo MCC

Tras finalizar con la fase 3 con éxito, se procedió a modificar el código implementado con el objetivo de permitir utilizar la base de datos al completo.

Estas pruebas realizaban la comparación de forma manual, es decir, el operario debía ir seleccionando cada muestra de una en una, cosa que para realizar un número tan elevado de comparaciones no era viable, por lo que se decidió modificar el código incluyendo un bucle que realizara de forma automática todas las comparaciones oportunas.

Aprovechando los recursos del entorno Visual Studio se realizó una aplicación de escritorio, o WPF, en la que de forma más óptima y sencilla, fuera capaz de realizar todas las comparaciones necesarias.

Fase final. Aplicación WPF

La aplicación desarrollada consta de una interfaz muy sencilla, se muestra en la figura 21, la cual permite seleccionar el algoritmo a utilizar y el sensor cuyas muestras se quieren comparar.

Una vez escogidos ambos requisitos, para comenzar a procesar las muestras simplemente hay que pulsar el botón START, y esperar hasta obtener uno de los dos mensajes posibles: "Procesado de [nombre del sensor] para el [nombre del algoritmo]... correcto!" en el caso de que el programa haya concluido de forma correcta escribiendo los ficheros correspondientes o "Error durante el procesado" en el caso de que ocurriera un error o excepción durante el procesado. Ambos casos se muestran en la figura 22 y 23, respectivamente.

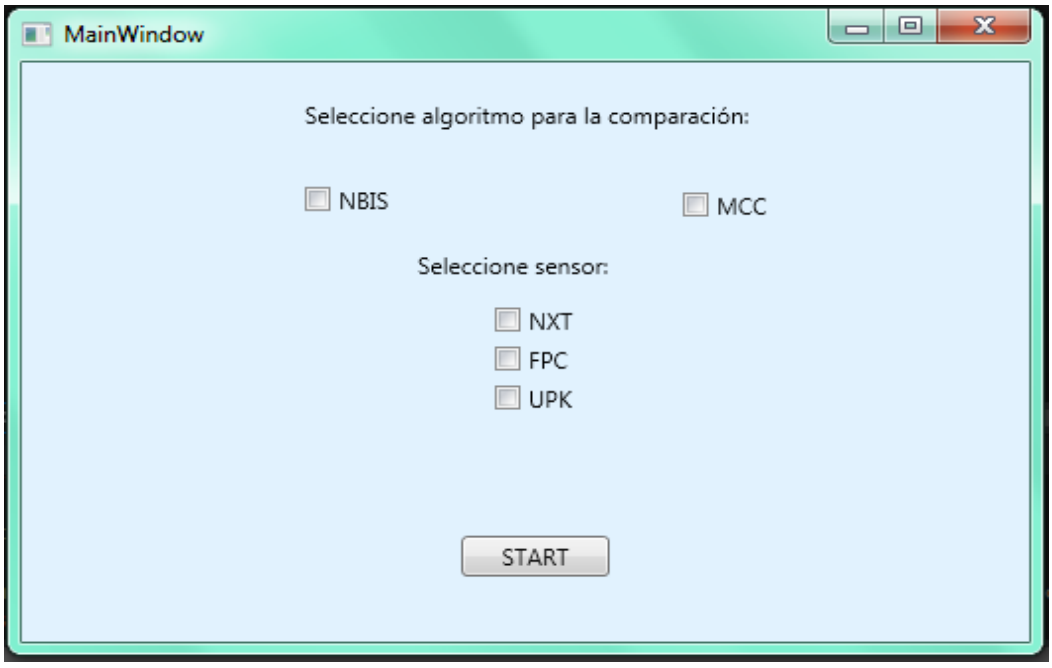

Figura 21. Aplicación WPF final para la comparación

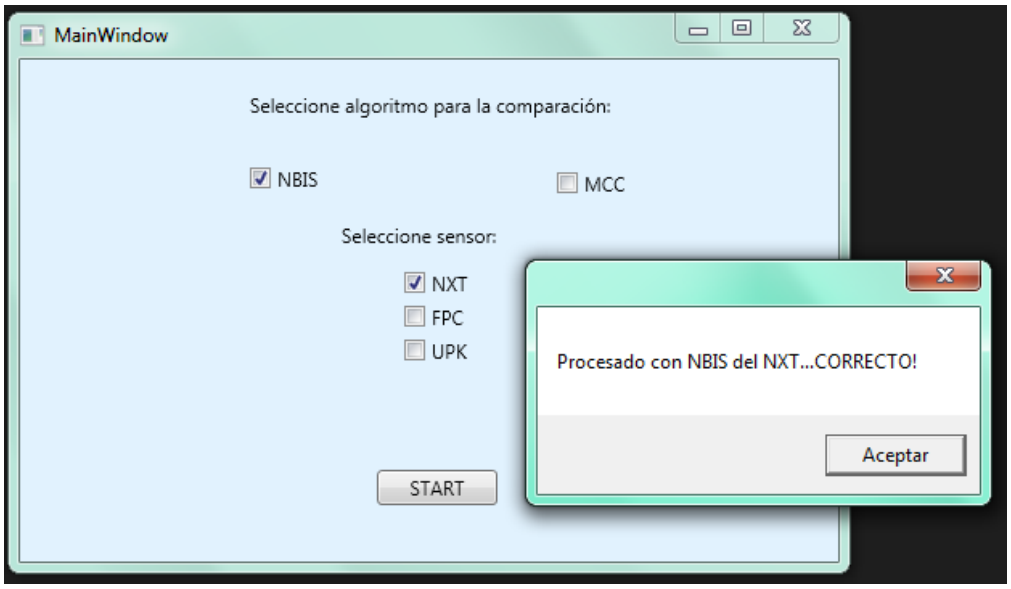

Figura 22. Mensaje de proceso completado

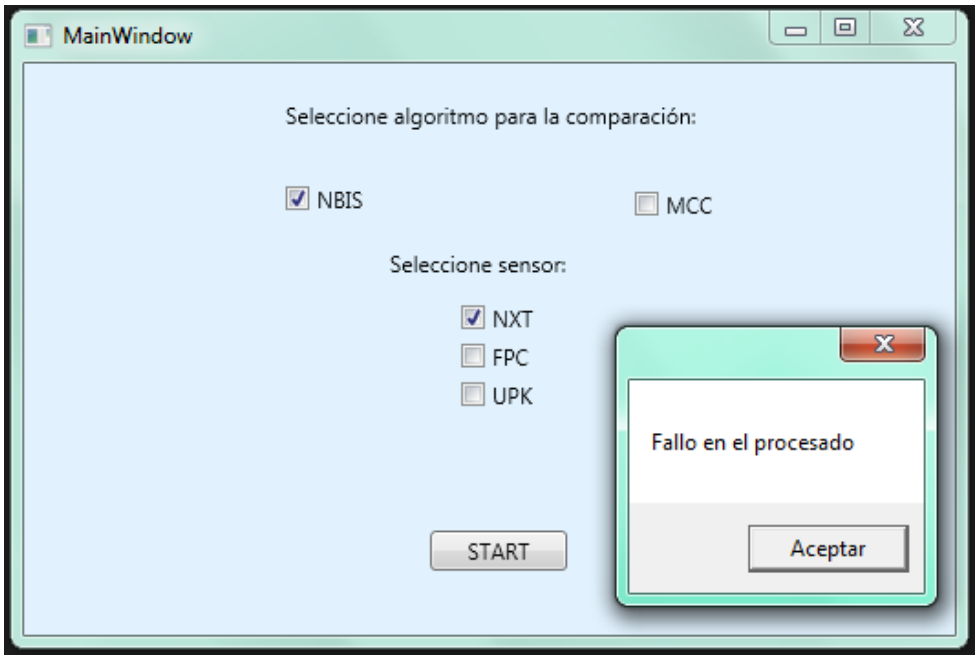

Figura 23. Mensaje de fallo durante el proceso de comparación

El funcionamiento y los procesos que sigue la aplicación de comparación tras ser pulsado el botón START se explicarán en los siguientes apartados.

4.1.1 Funcionamiento de la aplicación de comparación

La aplicación de comparación dispone de un total de ocho funciones para realizar las comparaciones oportunas y obtener los ficheros con los resultados.

Las funciones implementadas son:

Función para la comparación de las muestras de NXT bajo NBIS. bool comparacionNbisNXT( )

La llamada a esta función se realiza cuando se quiere procesar las muestras capturadas por el sensor NXT bajo el algoritmo NBIS.

La función devuelve un booleano, es decir, *true* o *false*, una vez terminadas todas las sentencias. Si el valor retornado es *true* el proceso ha concluido correctamente. Por el contrario, si es *false,* significa que ha ocurrido un problema durante la ejecución.

Dispone de seis variables principales: dos array de tipo *minutia* (Minutia[]) proporcionado o por la .DLL del software NBIS, uno para guardar las minucias correspondientes a la muestra 1 y otro para la muestra 2. Y cuatro objetos de tipo *bitmap:* en dos se cargan las muestras originales para la muestra 1 y 2, y en los otros dos se almacena la imagen procesada bajo las especificaciones requeridas por el software NBIS, que son: un tamaño de 8 bits con 256 niveles de gris.

Una vez declaradas las variables el programa accede al directorio donde se encuentran almacenadas las carpetas de los usuarios con sus correspondientes muestras.

Para el caso de la asignación de la muestra 1 se crea primeramente un vector en el que se almacena un máximo de seis muestras correspondientes a las imágenes de reclutamiento de los seis dedos de cada usuario. Una vez creado dicho vector, se asigna el primer objeto a la muestra 1, se procesa la imagen con las especificaciones disponibles y se detectan las minucias llamando a la función de NBIS *Nbis.DetectMinutiae.FromBitmap,* la cual rellena el vector de minucias para la muestra 1.

Después de disponer de las minucias para la imagen de reclutamiento del primer dedo se pasa a asignar una imagen a la muestra 2 correspondiente con las capturas de verificación de cada usuario. Y de igual manera que para la muestra 1 se procesa dicha imagen cargada para poner obtener el número de minucias y almacenarlo en el vector correspondiente.

Una vez que se dispone del número de minucias se llama a la función desarrollada por NBIS: *Nbis.Matcher.Compare,* la cual realiza la comparación devolviendo un entero correspondiente al resultado de la misma.

Este resultado es almacenado en el fichero *fGenuinos.txt* en el caso de que ambas muestras correspondan al mismo usuario y mismo dedo o en el fichero *fImpostores.txt* si las muestras corresponden a distintos usuarios.

Cuando se termina de comparar todas las imágenes del reclutamiento de un usuario con todas las imágenes de verificaciones de todos los usuarios, se repite el proceso hasta haber comparado todas las muestras de reclutamiento de todos los usuarios con todas las muestras de verificaciones de todos los usuarios.

Función para la comparación de las muestras de FPC bajo NBIS. bool comparacionNbisFPC( )

Esta función realiza las comparaciones oportunas de las muestras capturadas por el sensor FPC bajo el algoritmo NBIS.

Su funcionamiento es igual que para las muestras capturadas por el sensor NXT.

Función para la comparación de las muestras de UPK bajo NBIS. bool comparacionNbisUPK( )

La función realiza las comparaciones oportunas de las muestras capturadas por el sensor UPK bajo el algoritmo NBIS.

Su funcionamiento es igual que para las muestras capturadas por el sensor NXT y FPC.

Función para realizar la matriz de conversión de las muestras. Bitmap ImageMatrix (Bitmap oldImage)

La implementación de esta función fue necesaria dado que el software Nbis trabaja con imágenes de 8 bits y de 256 niveles de gris y no todas las imágenes capturadas cumplen con dichos requisitos. La función recibe como parámetro de entrada el bitmap que contiene la imagen original. Utilizando la función *ImageToMatrix*, de la librería Accord.Imaging, se transforma el bitmap de entrada en una matriz de 256 posiciones en las que se almacena el valor de cada píxel de la imagen y se vuelve a transformar a un nuevo bitmap, con la función *MatrixToImage*, de 8 bits.

Este bitmap generado se retorna a la función principal para ser usado y obtener las minucias correspondientes.

Función para la comparación de las muestras de NXT bajo MCC. bool comparacionMCC_NXT( )

La llamada a esta función se realiza cuando se quiere procesar las muestras capturadas por el sensor NXT bajo el algoritmo MCC.

La función devuelve un booleano, es decir, *true* o *false*, una vez terminadas todas las sentencias. Si el valor retornado es *true* el proceso ha concluido correctamente. Por el contrario, si es *false,* significa que ha ocurrido un problema durante la ejecución.

Al igual que las funciones para procesar con el algoritmo NBIS, esta función dispone de seis variables principales: dos vectores de tipo *minutia* (Minutia[]) proporcionado por la librería dinámica del software NBIS, uno para guardar las minucias correspondientes a la muestra 1 y otro para la muestra 2. Y cuatro objetos de tipo *bitmap:* en dos se cargan las muestras originales para la muestra 1 y 2, y en los otros dos se almacena la imagen procesada bajo las especificaciones requeridas por el software MCC, que son: un tamaño de 8 bits y 256 niveles de gris.

Para conseguir estos requisitos en las muestras se utiliza la función implementada, y comentada anteriormente, *ImageMatrix.*

Para realizar la comparación MCC SDK utiliza plantillas. Para generarlas dispone de la función MccSdk.CreateMccTemplate, pero esta necesita que se le pase el vector con las minucias correspondientes de la muestra y no dispone de su propio extractor, por lo que se utiliza el del software NBIS.

La forma de representar las minucias no es igual para NBIS que para MCC por lo que es necesario implementar una función que convierta las minucias del "tipo" NBIS a MCC. Esta función es la *coversionArray*.

De igual manera que para el algoritmo NBIS esta función accede al directorio donde se encuentran almacenadas las muestras de los usuarios, y realiza la asignación de las capturas para las muestras 1 y 2.

Tras crear las plantillas correspondientes se llama a la función *MccSdk.MatchMccTemplates* la cual realiza la comparación y devuelve el valor resultante. Este valor es almacenado en el fichero *fGenuinos.txt* en el caso de tratarse del mismo usuario y el mismo dedo para ambas muestras, o en *fImpostores.txt* si se trata de usuarios distintos.

Cuando se termina de comparar todas las imágenes del reclutamiento de un usuario con todas las imágenes de verificaciones de todos los usuarios, se repite el proceso hasta haber comparado todas las muestras de reclutamiento de todos los usuarios con todas las muestras de verificaciones de todos los usuarios.

A diferencia que el NBIS, el MCC no permite realizar la comparación de una muestra que no disponga de ninguna minucia, es decir, tras la extracción de las minucias el array sigue estando vacío: es *null,* por lo que las capturas que no disponen de minucias se almacenan en un fichero para poder llevar la cuenta del número total de muestras a la que les ocurre esto, dado que es el error conocido como FTA.

Función para la comparación de las muestras de FPC bajo MCC. bool comparacionMCC_FPC( )

Esta función realiza las comparaciones oportunas de las muestras capturadas por el sensor FPC bajo el algoritmo MCC.

Su funcionamiento es igual que para las muestras capturadas por el sensor NXT.

Función para la comparación de las muestras de UPK bajo NBIS. bool comparacionMCC_UPK( )

La función realiza las comparaciones oportunas de las muestras capturadas por el sensor UPK bajo el algoritmo MCC.

Su funcionamiento es igual que para las muestras capturadas por el sensor NXT y FPC.

Función para realizar la conversión del vector de minucias del formato NBIS al MCC. List <Minutia> conversionArray(Minutia[] arrayMinutia)

Esta función recibe como parámetro el vector de minucias en formato de NBIS, y devuelve una lista, para su posterior conversión a un vector, cuyo contenido son las minucias de la muestra en el formato MCC.

Para ello se utiliza un bucle que lee una a una cada minucia y realiza el cambio de formato.

El formato de representación de minucias de NBIS y MCC viene explicado en el Anexo III de este documento.

4.2 Desarrollo de la aplicación para la obtención de los resultados gráficos

Como se explica en el apartado 3.5, esta aplicación se basa en el procesado de los ficheros obtenidos en la aplicación de comparación.

La elección del entorno para realizar la aplicación y procesar los ficheros obteniendo las gráficas deseadas, ha sido MATLAB: una herramienta de software matemático que ofrece un entorno de desarrollo integrado y un lenguaje de programación propio: .m [40].

Las gráficas deseadas son las correspondientes a las curvas utilizadas para el análisis de un rendimiento biométrico, a saber: gráfica FMR frente FNMR, curva DET y curva ROC.

Para realizar el procesado de los ficheros, genuinos e impostores, se disponía de la herramienta "EER_DET_conf.m" implementada por BioSecure.

El programa venía de forma genérico por lo que era necesario asignar los parámetros necesarios para cada variable. Una vez realizados todos los ajustes pertinentes se ejecuta.

Tras la finalización de la ejecución se obtiene como resultado el valor del EER, además de las gráficas FMR vs FNMR, curva DET y curva ROC.

4.2.1 Funcionamiento de EER_DET_conf.m

Esta función implementada en el entorno MatLab, está constituida por varias funciones.

La llamada a la función para obtener las gráficas pertinentes se realiza de la siguiente manera:

[EER] = EER DET conf (clients, imposteurs, OPvalue, pas0), donde:

- **clients** es un vector que guarda los resultados obtenidos para genuinos.
- **imposteurs** es un vector que guarda los resultados obtenidos para impostores.
- **OPvalue** es el valor de FMR (en porcentaje) para el cual se estima el valor del punto de operación (el punto de operación se define en términos de FNMR (en %) para un FMR fijado).
- **pas0** es el número de umbrales utilizados para calcular las distribuciones de los resultados.

Esta herramienta ofrece varios valores de salida, pero para este estudio solo es necesario la obtención del EER.

Este estudio se ha realizado fijando el **OPvalue** a 100 y el **pas0** a 1000.

CAPÍTULO 5. RESULTADOS

El presente capítulo está destinado a la exposición de los resultados obtenidos durante el experimento, junto con las explicaciones oportunas acerca de cada uno de ellos.

Se presentan los resultados por sensor y algoritmo, además de realizar una comparativa final entre los tres sensores trabajando con ambos algoritmos analizados.

5.1 Resultados de comparación para las muestras capturadas con el sensor NXT

La realización de las pruebas para el sensor NXT se han llevado a cabo con el número de comparaciones que aparecen en la tabla 4, las cuales se dividen entre comparaciones genuinas e impostoras para ambos algoritmos analizados.

Tabla 4. Número de comparaciones realizadas para el sensor NXT

	NBIS	MCC
Comparaciones genuinas	3906	3867
Comparaciones impostoras	1223314	1215367

En los siguientes apartados se presentarán las gráficas resultantes para cada algoritmo trabajando con el sensor NXT.

5.1.1 Con algoritmo NBIS

La figura 24 muestra la gráfica FMR frente FNMR, el eje de abscisas tiene un rango de 0 a 300, correspondiente al resultado de comparación de muestras con el que trabaja el algoritmo NBIS. EL eje de ordenadas representa la probabilidad con la que se puede dar un FNMR o un FMR para cada resultado de comparación.

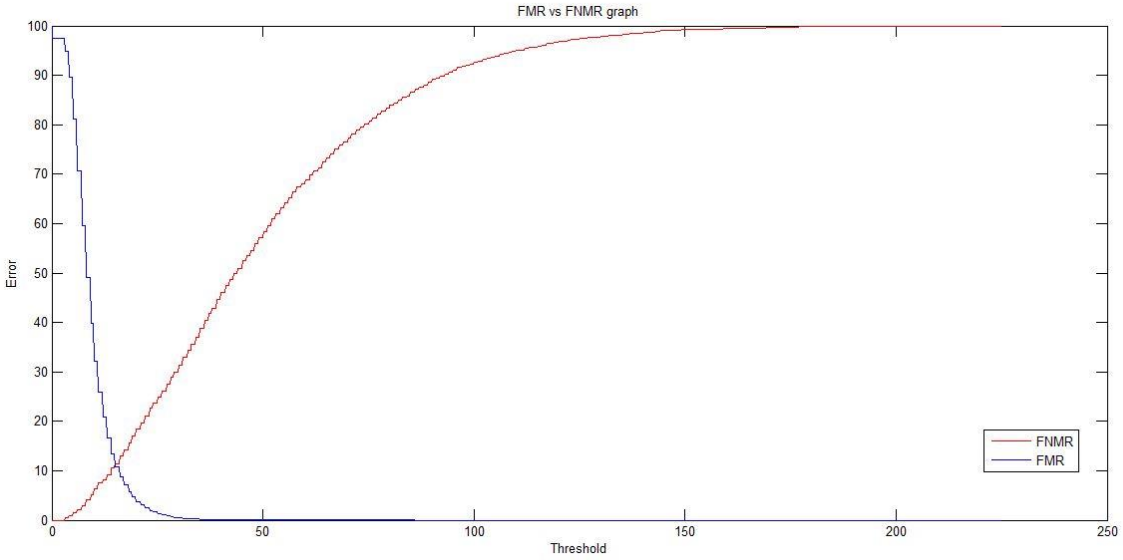

Figura 24. Gráfica FMR frente FNMR del NXT con el NBIS

En la figura 25 se encuentra un zoom de la zona más representativa de esta gráfica, que es el punto en el que se cortan las curvas FNMR y FNR, ese punto es el denominado EER y en este caso corresponde con un valor del 11.1794 %.

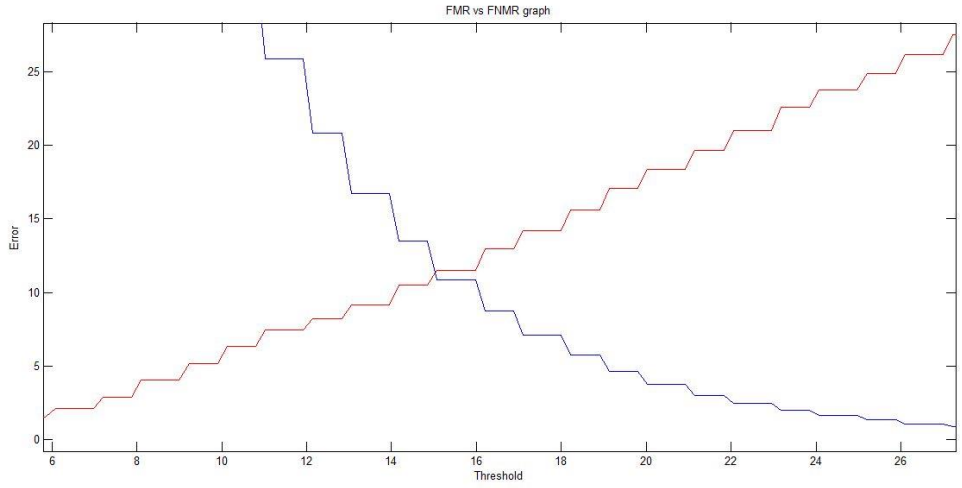

Figura 25. Zoom gráfica FMR vs FNMR del NXT con el NBIS

5.1.2 Con algoritmo MCC

Al igual que en el apartado anterior, las figuras 26 y 27 representan la gráfica FMR frente FNMR y el zoom de la zona representativa, respectivamente, para el algoritmo MCC.

En este caso el eje de abscisas trabaja en un rango de 0 a 1, correspondiente al rango de posibles resultados de comparación aportados por el algoritmo MCC.

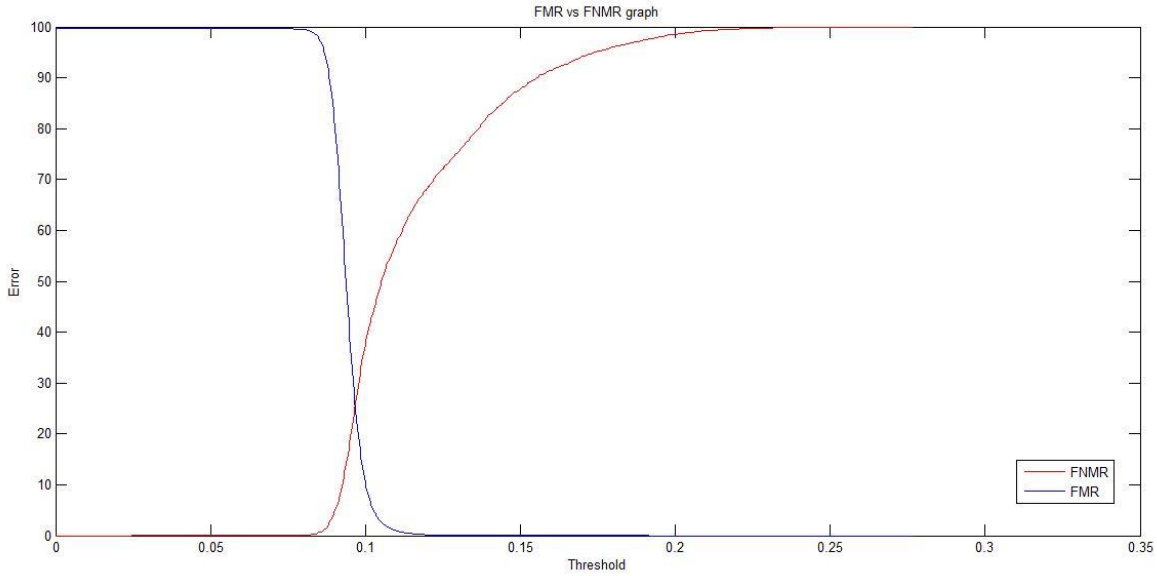

Figura 26. Gráfica FMR frente a FNMR del NXT con el MCC

El valor del EER es de un 25.3153 %, como se observa en la figura 27.

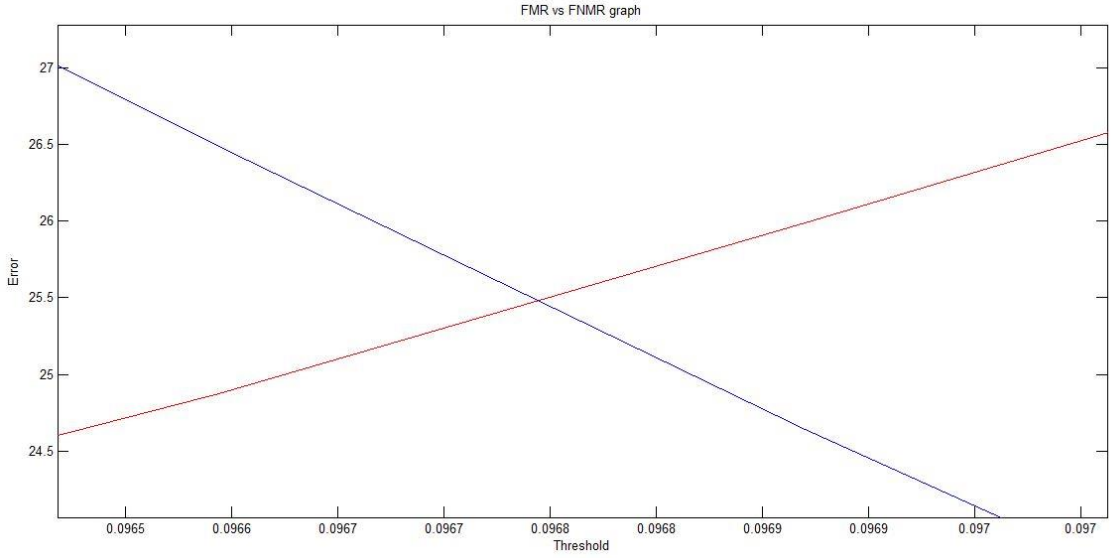

Figura 27. Zoom gráfica FMR frente a FNMR del NXT con el MCC

5.1.3 Representación para los dos algoritmos

A continuación se presenta una comparativa de ambos algoritmos trabajando con el sensor NXT. Esta comparativa se realiza sobre la curva DET, que como se ha explicado en el apartado 2.1.5, representa la desviación estándar de las probabilidades de error de falso rechazo frente a las de falsa aceptación, es decir, FNMR frente a FMR.

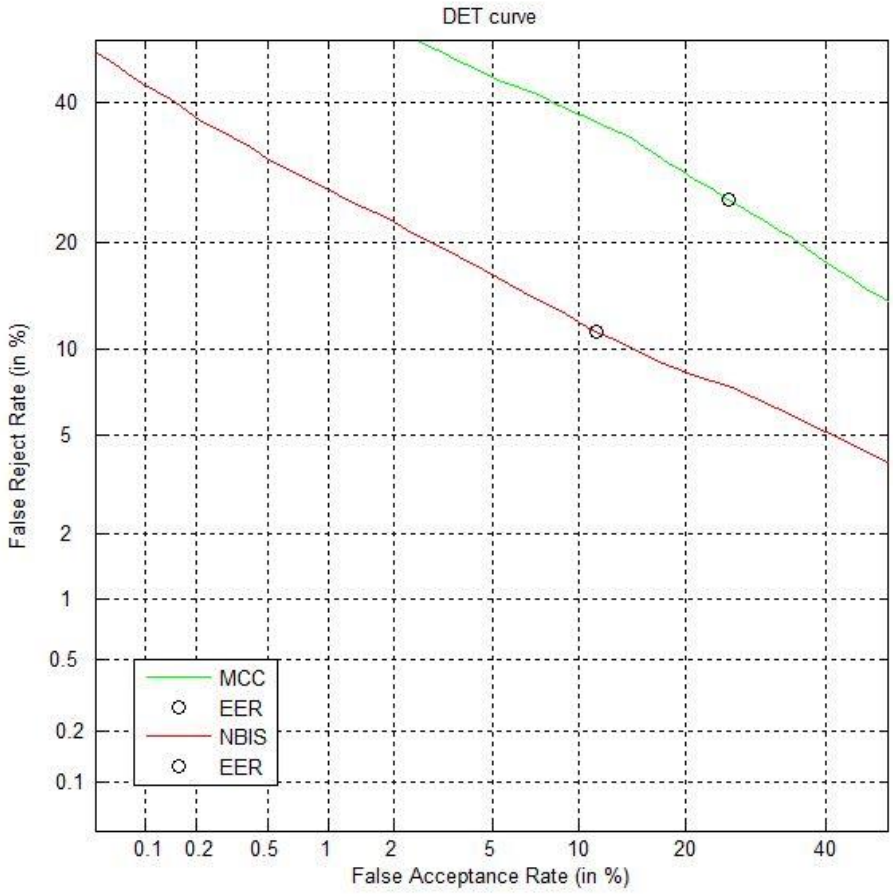

Figura 28. Curva DET del NXT con el NBIS y el MCC

Como se puede observar en la figura 28, el EER para el NBIS es menor que para el MCC, por lo que la curva de este está más próxima a la esquina inferior izquierda, lo que indica un mejor funcionamiento del sensor con el algoritmo NBIS que con el MCC.

En la tabla 5 se muestran el número de errores FTA y la probabilidad de error FTA, para ambos algoritmos, este último se calcula dividiendo el primero entre el número total de intentos y multiplicándolo por cien.

Tabla 5. Errores FTA para las muestras del sensor NXT

	NBIS	MCC
Número de intentos totales	4196	4157
Número de errores FTA	290	290
Número de intentos válidos	3906	3867
Probabilidad de error FTA rate	6.91 %	6.97%

En la tabla 6 se encuentra el número de errores FNMR y la probabilidad de que exista, para ambos algoritmos. La probabilidad se calcula dividiendo el número total de errores FNMR entre el número total de intentos y multiplicando por cien.

Tabla 6. Errores FNMR para las muestras del sensor NXT

	NBIS	MCC
Número de intentos totales	3906	3867
Número de errores FNMR	75	12
Número de intentos válidos	3831	3855
Probabilidad de FNMR	1.92%	0.31%

La tabla 7 muestra el EER para ambos algoritmos, y como se puede observar es mayor para el MCC, coincidiendo con la representación gráfica del mismo mediante distintas curvas.

Tabla 7. Valor del EER para el sensor NXT

	NBIS	MCC
EER	11.1794%	25.3153%

5.2 Resultados para las muestras capturadas con el sensor FPC

La realización de las pruebas para el sensor FPC se han llevado a cabo con el número de comparaciones que aparecen en la tabla 8, las cuales se dividen entre comparaciones genuinas e impostoras para ambos algoritmos analizados.

Tabla 8. Número de comparaciones realizadas para el sensor FPC

	NBIS	**MCC**
Comparaciones genuinas	4025	3062
Comparaciones impostoras	1277190	984502

En los siguientes apartados se presentarán las gráficas resultantes para cada algoritmo trabajando con el sensor FPC.

5.2.1 Con algoritmo NBIS

La figura 29 muestra la gráfica FMR frente FNMR, mientras que en la figura 30 se encuentra un zoom de la zona más representativa de esta gráfica: el EER. En este caso corresponde con un valor del 12.2005 %.

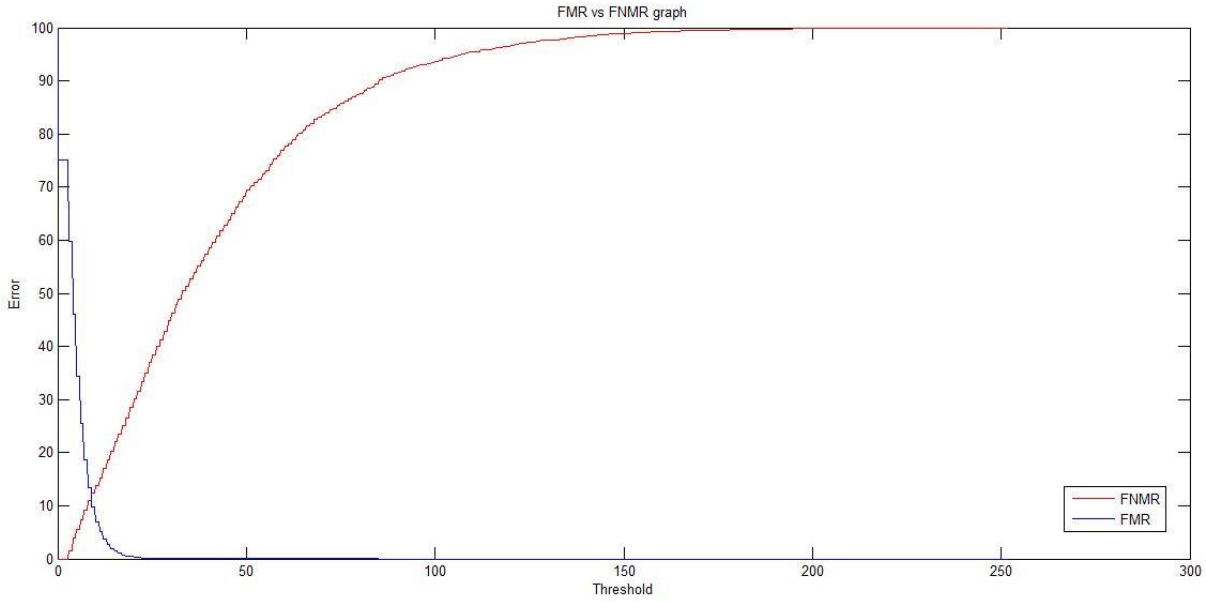

Figura 29. Gráfica FMR frente a FNMR del FPC con el NBIS

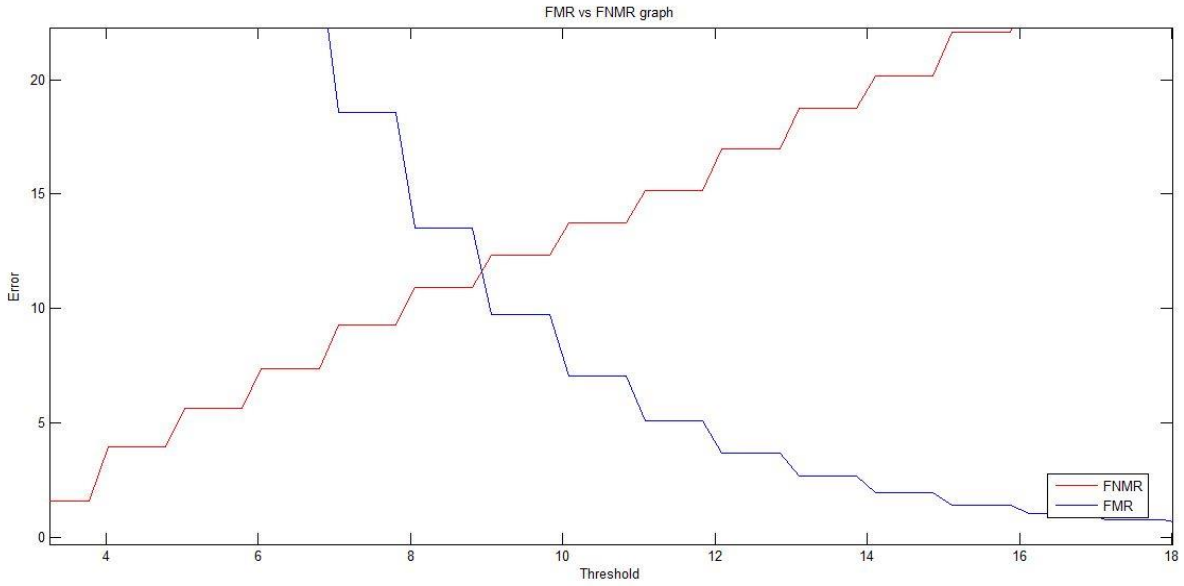

Figura 30. Zoom gráfica FMR frente a FNMR del FPC con el NBIS

5.2.2 Con algoritmo MCC

Al igual que en el apartado anterior, las figuras 31 y 32 representan la gráfica FMR frente FNMR y el zoom de la zona representativa, respectivamente, para el algoritmo MCC.

El valor del EER es de un 26.8959 %.

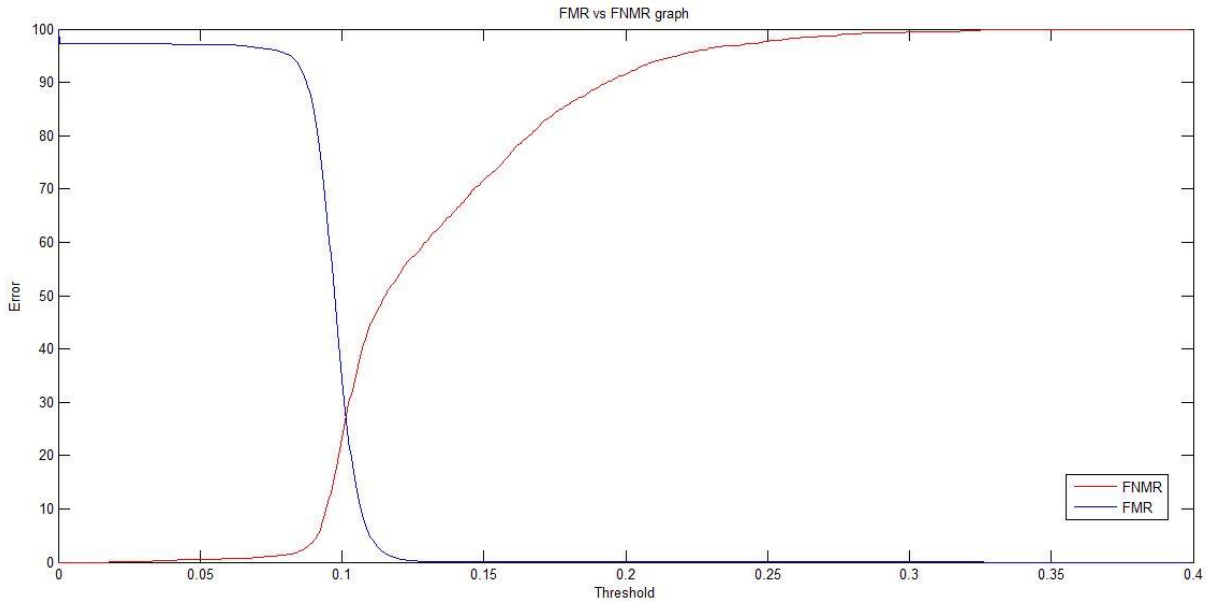

Figura 31. Gráfica FMR frente a FNMR del FPC con el MCC

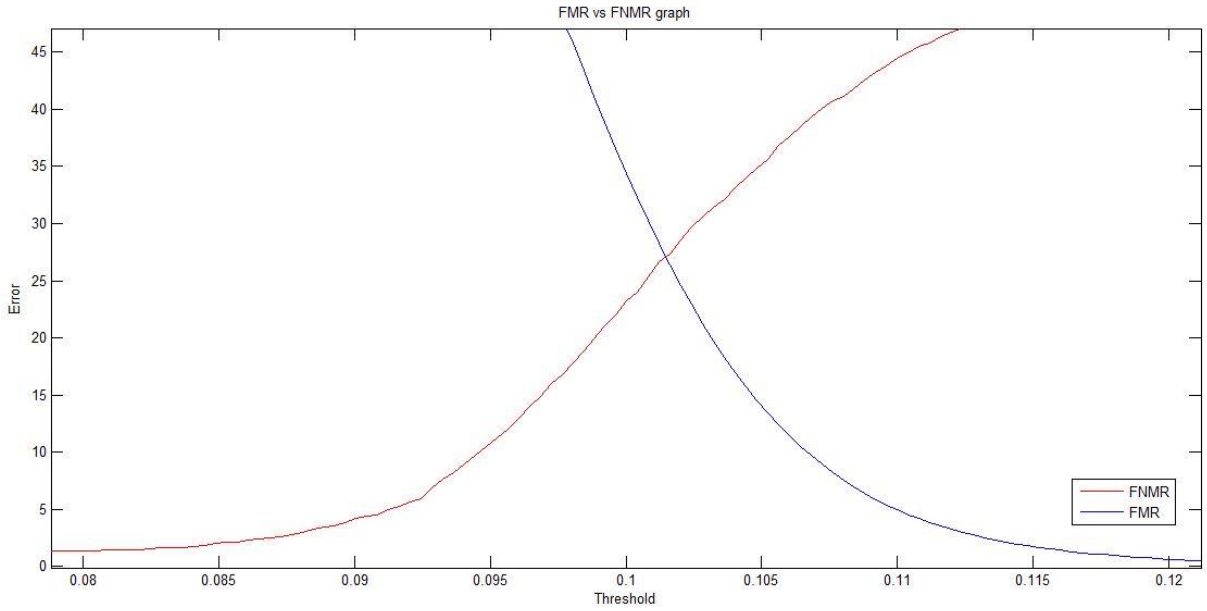

Figura 32. Zoom gráfica FMR frente a FNMR del FPC con el MCC

5.2.3 Representación para los dos algoritmos

En este apartado se presenta una comparativa de ambos algoritmos trabajando con el sensor FPC analizando la curva DET.

Como se puede observar en la figura 33, el EER para el NBIS es menor que para el MCC, por lo que la curva de este está más próxima a la esquina inferior izquierda, lo que indica un mejor funcionamiento del sensor con el algoritmo NBIS que con el MCC.

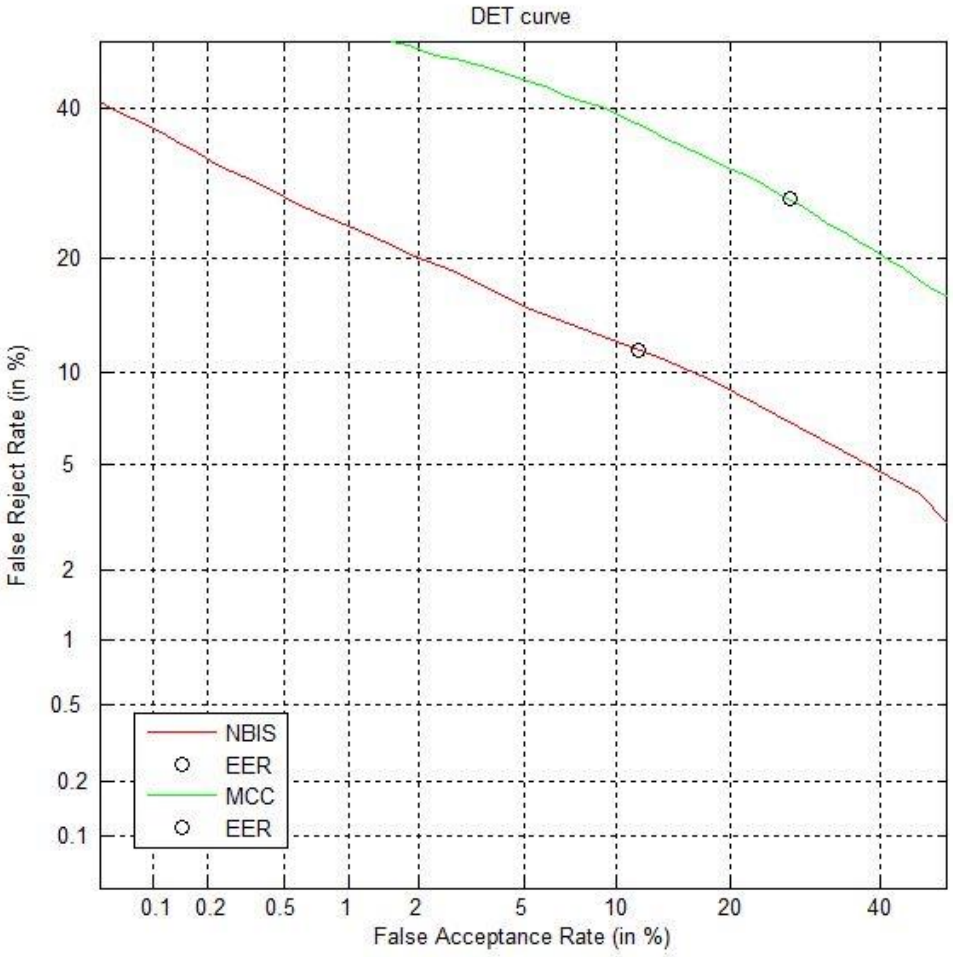

Figura 33. Curva DET del FPC con el NBIS y el MCC

En la tabla 9 se muestran el número de errores FTA y la probabilidad de error FTA, en la tabla 10 el número de errores FNMR y su probabilidad de error y en la tabla 11 el EER, todas ellas para ambos algoritmos.

Tabla 9. Errores FTA para las muestras del sensor FPC

	NBIS	MCC
Número de intentos totales	4324	3361
Número de errores FTA	299	299
Número de intentos válidos	4025	3062
Probabilidad de error FTA rate	6.91 %	8.89%

Tabla 10. Errores FNMR para las muestras del sensor FPC

	NBIS	MCC
Número de intentos totales	4025	3062
Número de errores FNMR	466	77
Número de intentos válidos	3559	2985
Probabilidad de FNMR	11.57%	2.51%

Tabla 11. Valor del EER para el sensor FPC

	NBIS	MCC
EER	12.2005%	26.8959%

5.3 Resultados para las muestras capturadas con el sensor UPK

La realización de las pruebas para el sensor UPK se han llevado a cabo con el número de comparaciones que aparecen en la tabla 12, las cuales se dividen entre comparaciones genuinas e impostoras para ambos algoritmos analizados.

Tabla 12. Número de comparaciones realizadas para el sensor UPK

	NBIS	MCC
Comparaciones genuinas	3898	3885
Comparaciones impostoras	1184770	1180598

En los siguientes apartados se presentarán las gráficas resultantes para cada algoritmo trabajando con el sensor UPK.

5.3.1 Con algoritmo NBIS

La figura 34 muestra la gráfica FMR frente FNMR, mientras que en la figura 35 se encuentra un zoom de la zona más representativa de esta gráfica: el EER. En este caso corresponde con un valor del 8.9753 %.

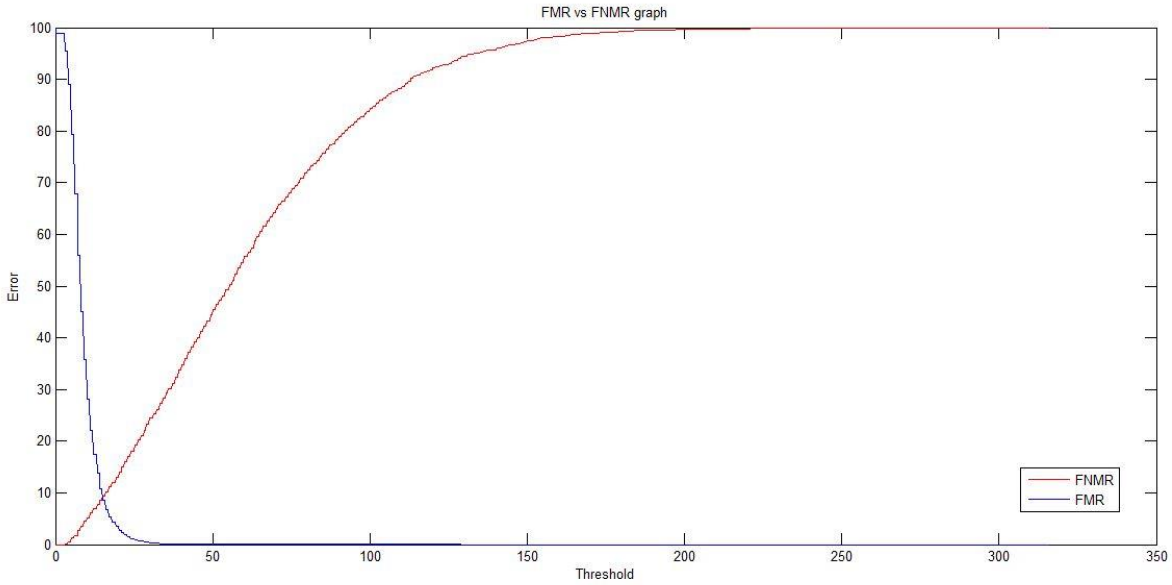

Figura 34. Gráfica FMR frente a FNMR del UPK con el NBIS

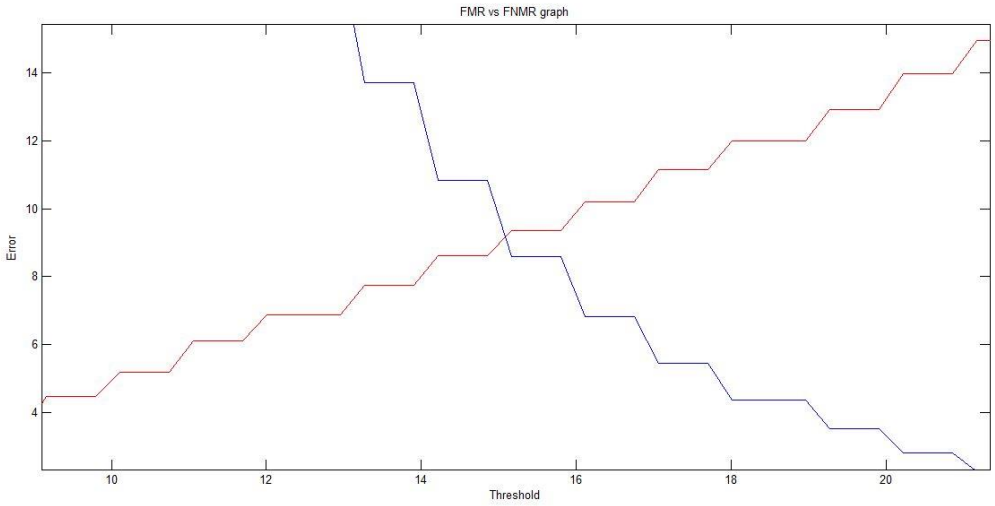

Figura 35. Zoom gráfica FMR frente a FNMR del UPK con el NBIS

5.3.2 Con algoritmo MCC

Al igual que en el apartado anterior las figuras 36 y 37 representan la gráfica FMR frente FNMR y el zoom de la zona representativa, respectivamente, para el algoritmo MCC.

El valor del EER es de un 22.7307 %.

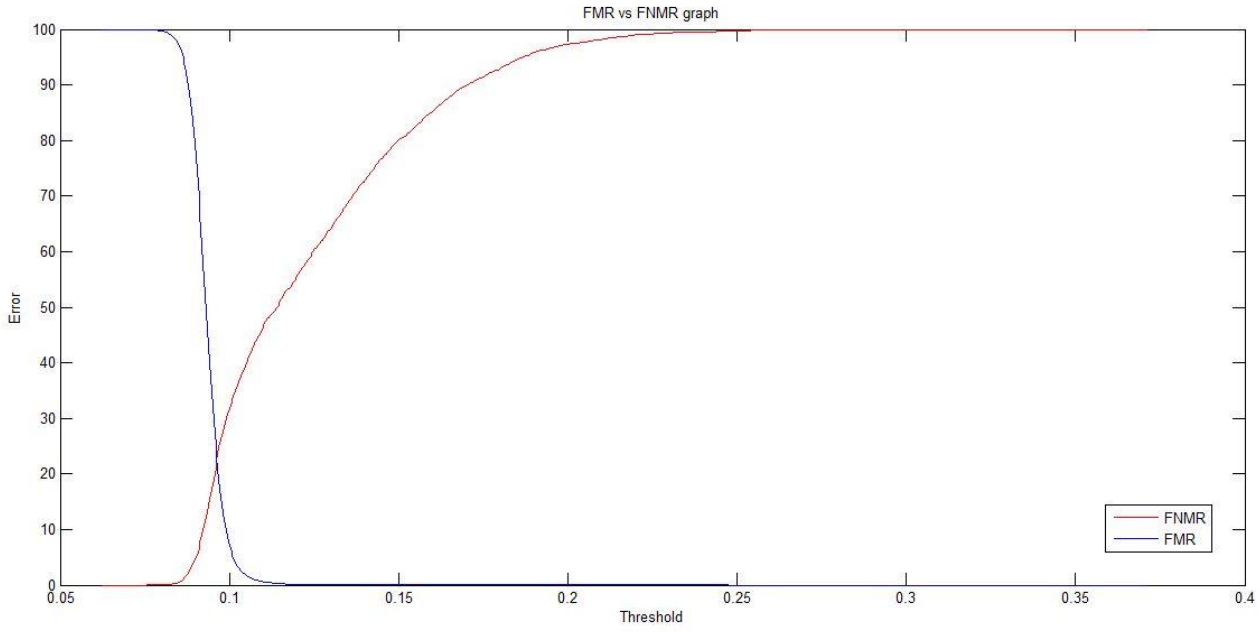

Figura 36. Gráfica FMR frente a FNMR del UPK con el MCC

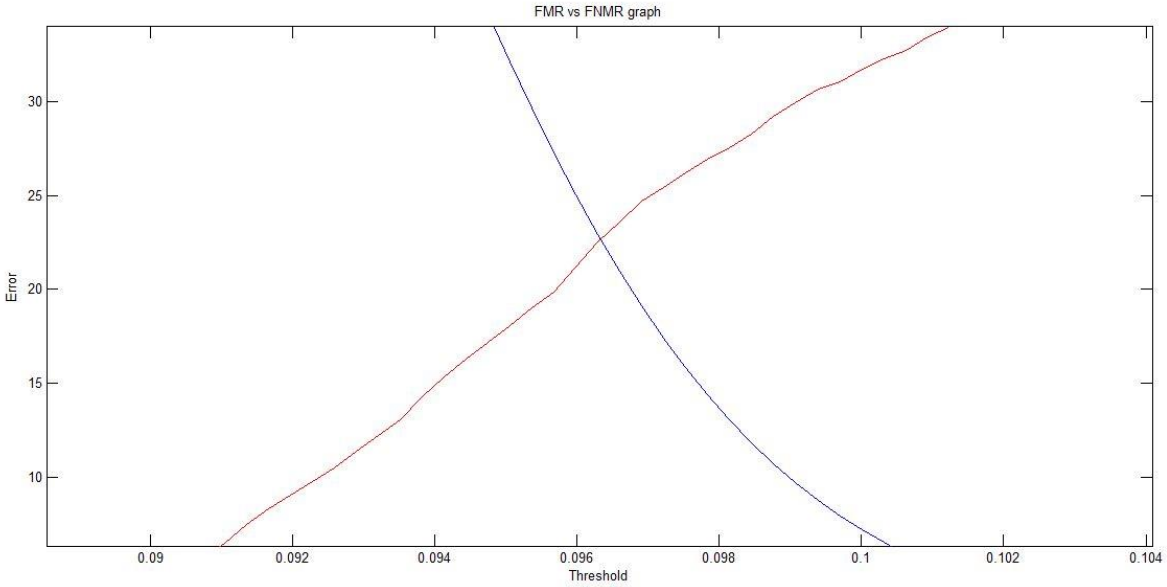

Figura 37. Zoom gráfica FMR frente a FNMR del UPK con el NBIS

5.3.3 Representación para los dos algoritmos

A continuación se presenta una comparativa de ambos algoritmos trabajando con el sensor UPK. En la figura 40 se muestra la curva DET.

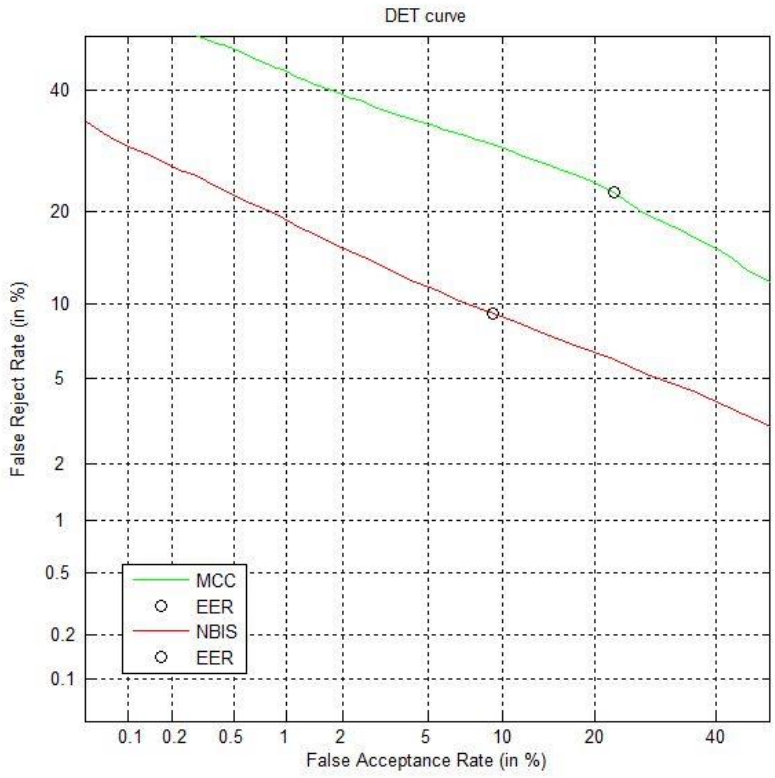

Figura 38. Curva DET del UPK con el NBIS y el MCC

Como se puede observar en la figura 38, el EER para el NBIS es menor que para el MCC, por lo que la curva de este está más próxima a la esquina inferior izquierda, lo que indica un mejor funcionamiento del sensor con el algoritmo NBIS que con el MCC.

En la tabla 13 se muestran el número de errores FTA y la probabilidad de error FTA, en la tabla 14 el número de errores FNMR y su probabilidad de error y en la tabla 15 el EER, todas ellas para ambos algoritmos.

Tabla 13. Errores FTA para las muestras del sensor FPC

	NBIS	MCC
Número de intentos totales	3898	3885
Número de errores FTA	283	283
Número de intentos válidos	3615	3602
Probabilidad de error FTA rate	7.26 %	7.28%

Tabla 14. Errores FNMR para las muestras del sensor FPC

	NBIS	MCC
Número de intentos totales	3898	3885
Número de errores FNMR	6	1
Número de intentos válidos	3892	3884
Probabilidad de FNMR	0.15%	0.02%

Tabla 15. Valor del EER para el sensor UPK

	NBIS	MCC
EER	8.9753%	22.7307%

5.4 Curva DET para los tres sensores

Este apartado está destinado a la representación de la curva DET para los tres sensores juntos, separados por algoritmo. Y una última gráfica en la que se encuentren los resultados de todos los sensores para ambos algoritmos.

5.4.1 Con algoritmo NBIS

En la figura 39 se muestra la curva DET para los tres sensores trabajando con el algoritmo NBIS. Como se puede observar la curva del NXT y del FPC son bastante similares, afirmación que es contrastada con los datos aportados en los apartados anteriores, mientras que la curva correspondiente al análisis de las muestras obtenidas por el sensor UPK, se aleja de ellas mostrando un mejor rendimiento.

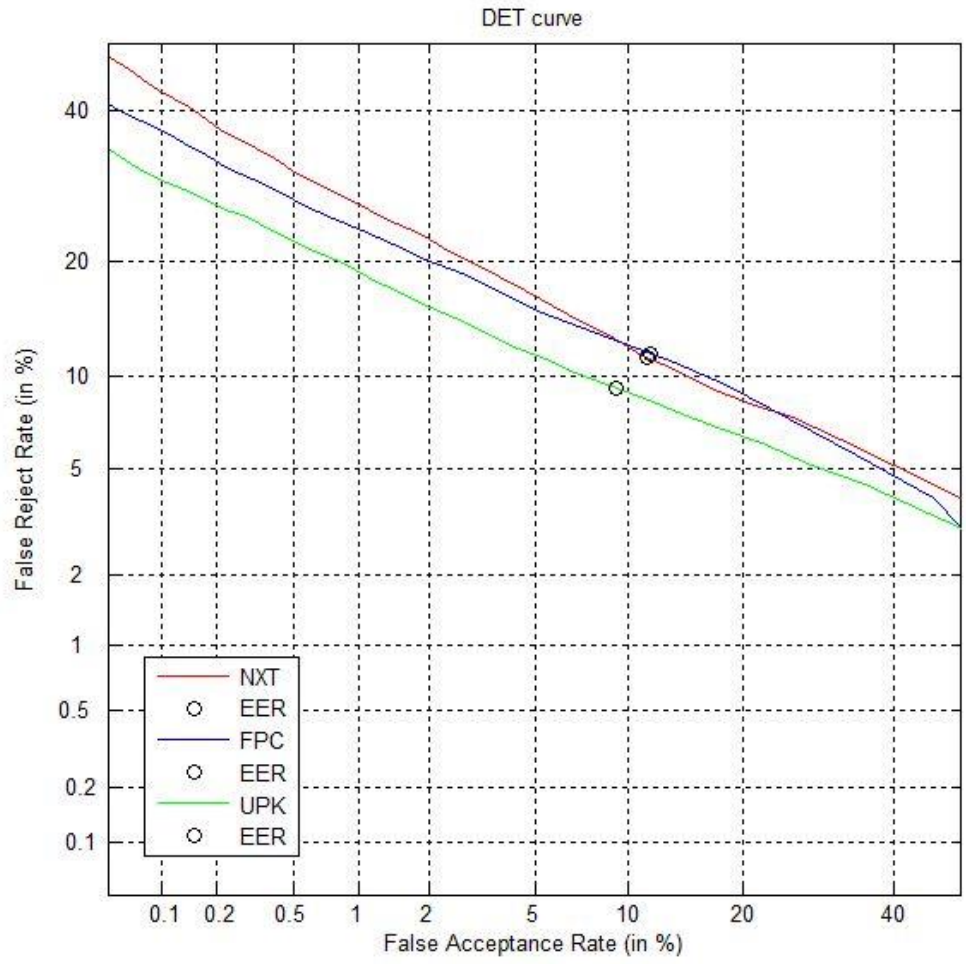

Figura 39. Curva DET para los tres sensores con el NBIS

5.4.2 Con algoritmo MCC

Al igual que en el apartado anterior, la figura 40 muestra la curva DET para los tres sensores trabajando con el algoritmo MCC.

En ella se puede observar que las curvas del NXT y FPC siguen prácticamente la misma trayectoria mientras que la del UPK se aleja de ellas, lo que indica que el rendimiento para este último sensor es mejor que para los primeros, al igual que ocurre para el algoritmo NBIS.

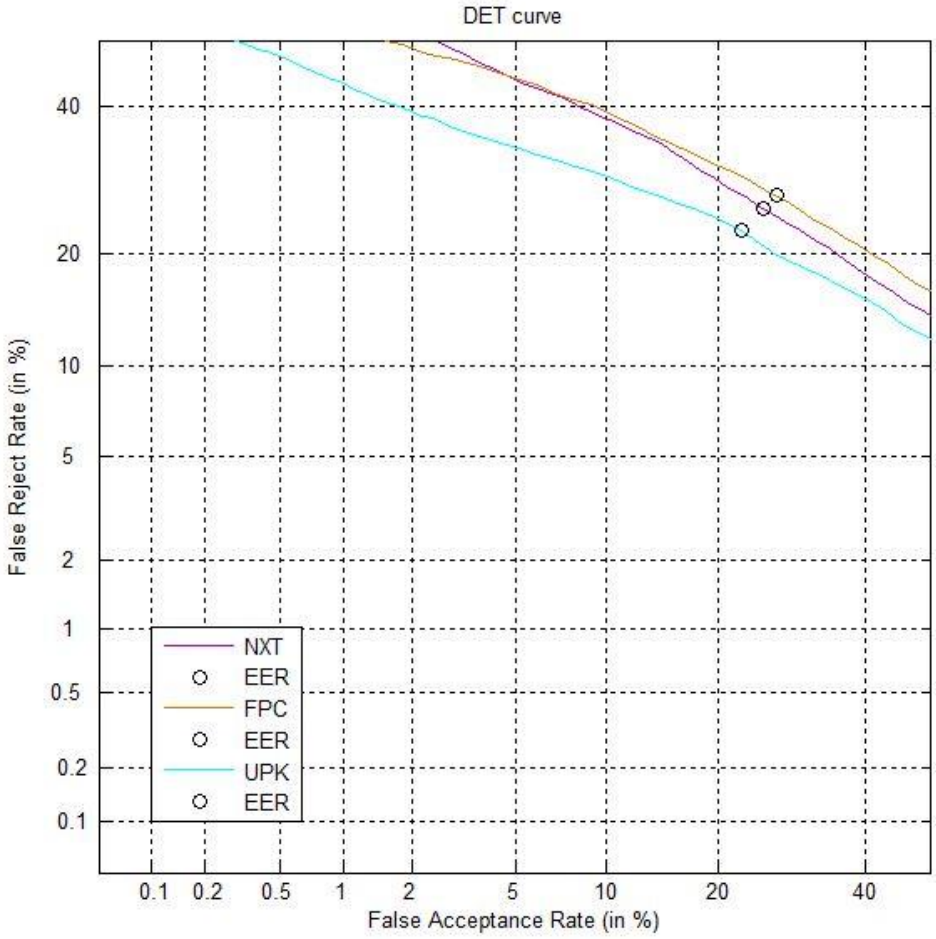

Figura 40. Curva DET para los tres sensores con el MCC

5.4.3 Representación para ambos algoritmos

En la figura 41 se muestra la curva DET para los tres sensores y ambos algoritmos. En ella se observa que las curvas que representan el trabajo bajo el algoritmo NBIS presentan un mejor resultado que para el MCC, siendo la mejor de las seis pruebas la realizada con las muestras obtenidas por el sensor UPK y procesadas con el algoritmo NBIS.

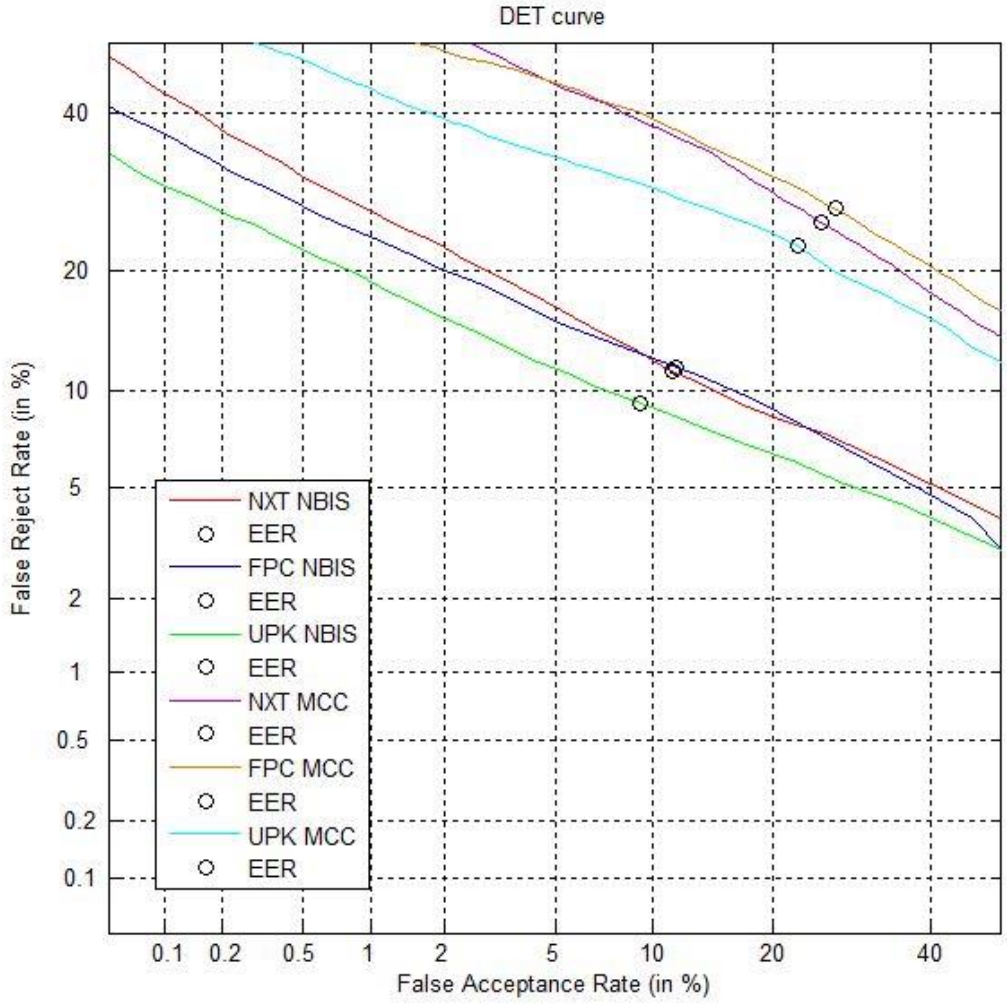

Figura 41. Curva DET para los tres sensores con ambos algoritmos

5.5 Curva ROC para los tres sensores

Este apartado está destinado a la representación de la curva ROC para los tres sensores juntos, separados por algoritmo. Y una última gráfica en la que se encuentren los resultados de todos los sensores para ambos algoritmos.

5.5.1 Con algoritmo NBIS

En la figura 42 se muestra la curva ROC para los tres sensores trabajando con el algoritmo NBIS. Como se puede observar, la curva del NXT y del FPC son bastante similares, afirmación que es contrastada con los datos aportados en los apartados anteriores, mientras que la curva correspondiente al análisis de las muestras obtenidas por el sensor UPK, se aleja de ellas mostrando un mejor rendimiento.

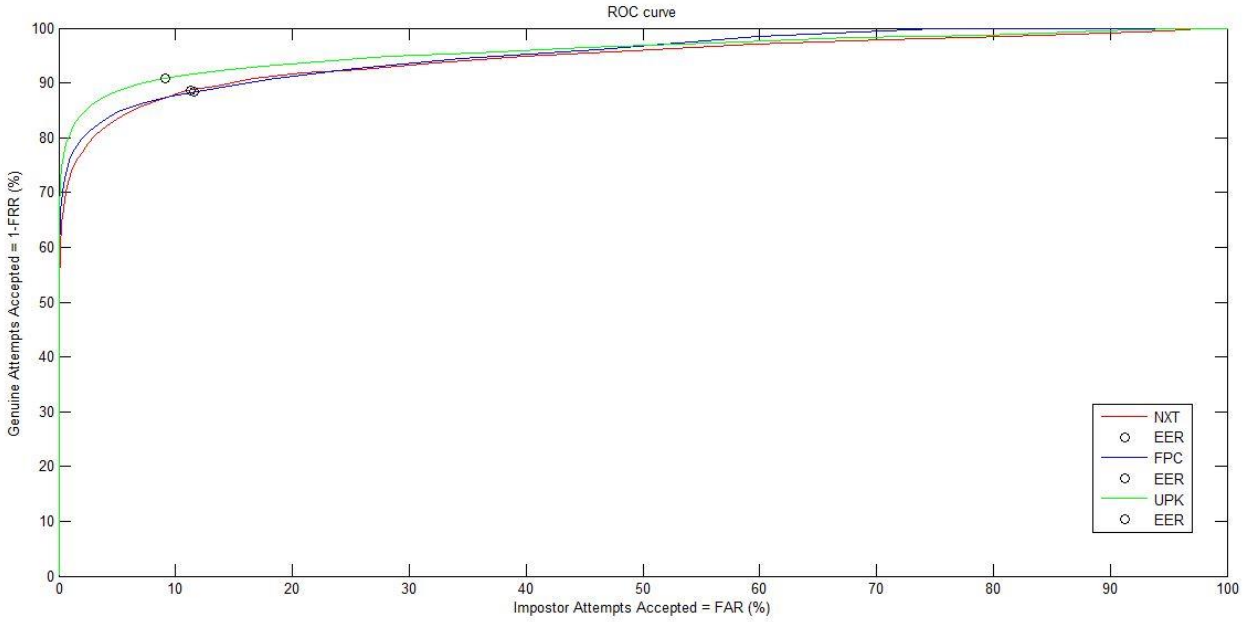

Figura 42. Curva ROC para los tres sensores con el NBIS

5.5.2 Con algoritmo MCC

Al igual que en el apartado anterior, la figura 43 muestra la curva ROC para los tres sensores trabajando con el algoritmo MCC.

En ella se puede observar que las curvas del NXT y FPC siguen trayectorias similares, mientras que la del UPK se aleja de ellas, lo que indica que el rendimiento para este último sensor es mejor que para los primeros, al igual que ocurre para el algoritmo NBIS.

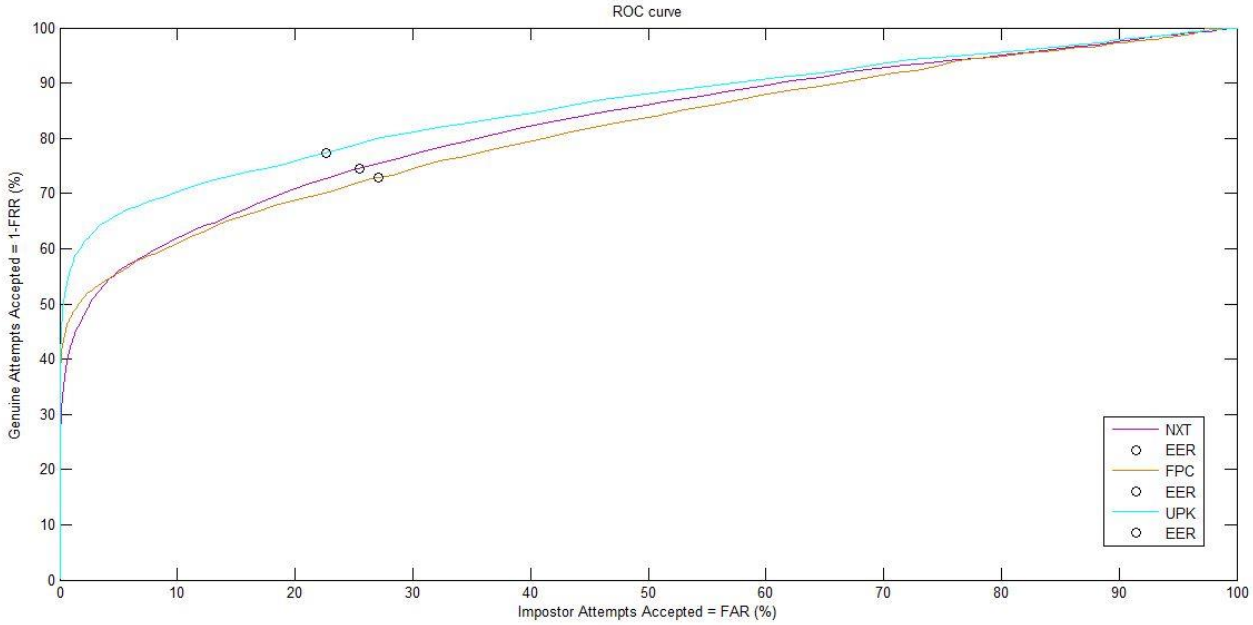

Figura 43. Curva ROC para los tres sensores con el MCC

5.5.3 Representación para ambos algoritmos

En la figura 44 se muestra la curva ROC para los tres sensores y ambos algoritmos. En ella se observa que las curvas que representan el trabajo bajo el algoritmo NBIS presentan un mejor resultado que para el MCC, siendo la mejor de las seis pruebas la realizada con las muestras obtenidas por el sensor UPK y procesadas con el algoritmo NBIS.

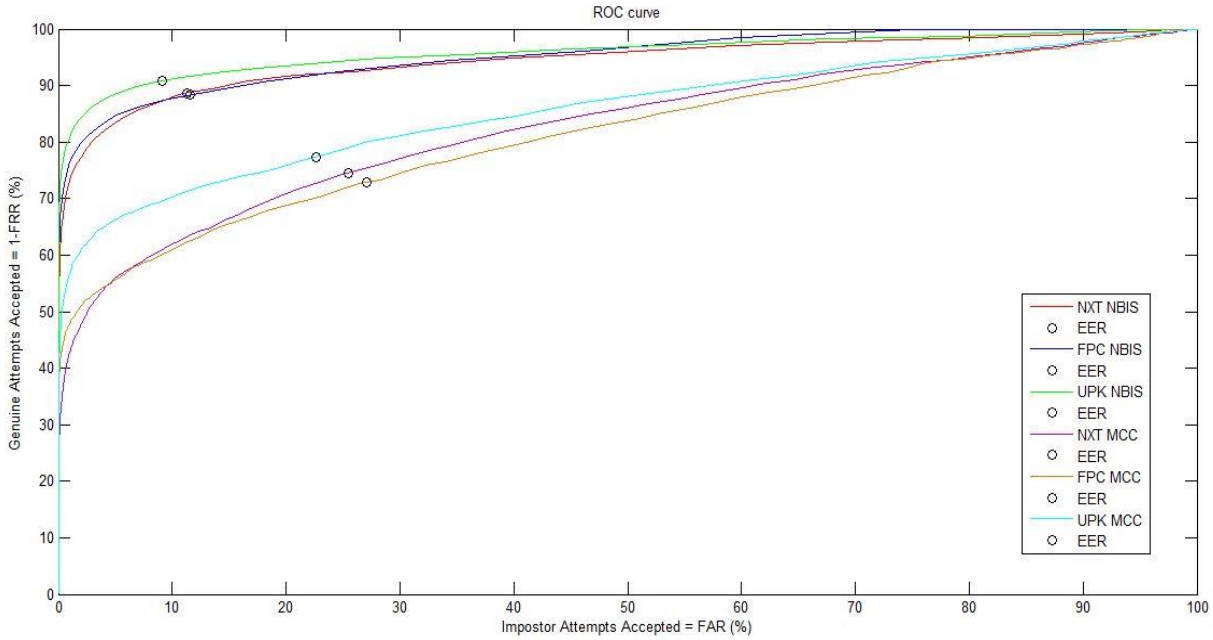

Figura 44. Curva ROC para los tres sensores con ambos algoritmos

CAPÍTULO 6. CONCLUSIONES Y LÍNEAS DE TRABAJO FUTURAS

Este capítulo corresponde al último del documento, dónde se hace referencia a las conclusiones tras la finalización del proyecto, tanto las generales respecto los objetivos marcados y las específicas de los resultados obtenidos.

También se dedica un último apartado destinado a las líneas de trabajo futuras tras la realización de éste Trabajo Fin de Grado.

6.1 Conclusiones

6.1.1 Conclusión general

La conclusión general acerca del trabajo realizado es positiva. Se puede afirmar haber cumplido con todos los objetivos marcados para el mismo, analizando la situación actual de esta tecnología y los medios existentes para su uso.

Se ha implementado correctamente una aplicación capaz de realizar las comparaciones de varias muestras obtenidas con tres sensores distintos y bajo el uso de dos algoritmos diferentes. Además de haber implementado otra aplicación encargada de analizar los resultados obtenidos y aportar las medidas de rendimiento.

Con el desarrollo de ambas aplicaciones se consigue cumplir con los objetivos marcados para este proyecto en el que se debía realizar una evaluación de rendimiento tecnológica sobre dos algoritmos, efectuando un posterior análisis de los resultados obtenidos.

Además se ha comprobado que un sistema electrónico no depende únicamente de la tecnología en la que se base el hardware del mismo, sino que también es igual de importante el software y la aceptación del cliente o usuario final.

6.1.2 Conclusión de los resultados obtenidos

El estudio está realizado bajo una base de datos reducida, por lo que el número de muestras utilizadas es menor. Lo ideal hubiera sido utilizar la base de datos al completo, dado que la biometría se basa en probabilidad, pero el coste computacional hubiese sido demasiado elevado. Aun así para realizar un primer estudio y obtener unos resultados orientativos con la base de datos reducida ha sido suficiente.

Como ya se ha comentado en el capítulo 5, correspondiente a los resultados obtenidos, si se analizan los resultados por sensor, se obtienen los mejores para el sensor UPK, seguido del NXT y por último el FPC.

En cambio, analizando los algoritmos se obtienen mejores resultados para el NBIS que para el MCC.

Atendiendo únicamente a los resultados de este estudio, sin analizar el entorno o aplicación real, el sistema de reconocimiento de huella dactilar óptimo sería el constituido por el sensor UPK trabajando bajo el algoritmo NBIS.

6.2 Líneas de trabajo futuras

Tras la realización de este proyecto, sería interesante continuar la línea de investigación, continuando con el estudio, analizando las tasas de throughtput o la diferencia entre utilizar algoritmos públicos y los disponibles en el mercado. De esta manera se podrían contrastar los resultados obtenidos en este estudio.

También, sería interesante implementar un sistema de reconocimiento biométrico de huella dactilar para una aplicación real. Esta aplicación podría ser el control de acceso de una oficina o la validación para poder hacer uso de un ordenador.

Con este sistema se podría comprobar si los resultados coinciden con los teóricos obtenidos en este trabajo, en el que el mejor rendimiento se da para el sensor UPK trabajando con el algoritmo NBIS, o por el contrario difieren y aportan resultados distintos.

BIBLIOGRAFÍA

[1] Biometrics History. http://www.biometrics.gov/documents/biohistory.pdf, consultado: "Julio 2015"

[2] Evaluación de parámetros de rendimiento en dispositivos biométricos. Septiembre 2010.

[3] Historia de la biometría. http://www.biometria.gov.ar/acerca-de-la-biometria/historia-de-la-biometria.aspx, consultado: "Julio 2015"

[4] Ted Dunstone; Neil Yager, Biometric System and Data Analysis; Design, Evaluation and Data Mining. Springer, p. 15.

[5] Imagen recuperada de : http://americas.probayes.com/store/index.php?main_page=product_info&products_id=9

[6] Imagen recuperada de: http://ee.capasso.co/articulo/1306/firma-electronica-y-firma-digital-ii

[7] ISO/IEC JTC1/SC37 Biometrics, "SC37 Standing Document 11(SD11), Part 1 Harmonization Document, Mayo 2008.

[8] Ted Dunstone; Neil Yager, Biometric System and Data Analysis; Design, Evaluation and Data Mining. Springer.

[9] Ted Dunstone; Neil Yager, Biometric System and Data Analysis; Design, Evaluation and Data Mining. Springer, p. 113.

[10] Imagen recuperada de: http://deducimos.blogspot.com.es/2012/11/las-huellas-dactilares.html

[11] Imagen recuperada de: http://www.avalonred.com/la-biometria-como-clave-para-la-seguridad/

[12] Francis Galton (1892), Fingerprints, MacMillan and CO.

[13]http://dis.um.es/~lopezquesada/documentos/IES_1213/SAD/curso/UT3/ActividadesAlumnos/12/enlaces/biometricos.html

[14] Imagen recuperada de: http://www.dolthink.com/minucias-y-huellas-dactilares.html

[15] García, F. (2014). Mejora de algoritmos de reconocimiento de huellas dactilares en entornos forenses (Proyecto Fin de Carrera). Universidad Autónoma, Madrid.

[16] Lindoso, A. (2009) Contribución al reconocimiento de huellas dactilares mediante técnicas de correlación y arquitecturas hardware para el aumento de prestaciones (Tesis Doctoral). Universidad Carlos III, Madrid

[17] Cómo funcionan los lectores de huella digital. http://tec-mex.com.mx/promos/bit/bit0903-bio.htm, consultado: "Julio 2015"

[18] Tipos de lectores de huellas dactilares. http://www.guiaspracticas.com/controles-de-acceso/tipos-de-lectores-de-huellas-dactilares, consultado "Julio 2015"

[19] Real Academia Española. http://www.rae.es/

[20] Algoritmo. http://www.innovatrics.com/es/tecnologia/algoritmo, consultado: "Agosto 2015"

[21] National Institute of Standards and Technology; User's Guide to NIST Biometric Image Software (NBIS).

[22] National Institute of Standards and Technology; User's Guide to NIST Biometric Image Software (NBIS), p. 67.

[23] National Institute of Standards and Technology; User's Guide to NIST Biometric Image Software (NBIS), p. 78.

[24] Biometric System Laboratory; MCC Software Development Kit (SDK), version 2.0; Documentation.

[25] Imagen recuperada de : http://biolab.csr.unibo.it/research.asp?organize=Activities&select=&selObj=81&pathSubj=111||8||81&Req=&

[26] Fernández, Dr. B. (2015). Performance testing evaluation report of results. Recuperado de http://idtestinglab.uc3m.es/data/_uploaded/Publications/PUBLIC%20REPORT_589%20users_Fingerprint_v1_1_release.pdf

[27] Imagen recuperada de: http://nextbiometrics.com/products/for_notebooks___tablets/the_nb-3010-u__the_oyster_/

[28] http://www.fingerprints.com/wp-content/uploads/2013/08/720-FPC1011F3_A_Product-sheet.pdf

[29] Imagen recuperada de: http://www.biometricsupply.com/res/upek-eikon-touch-300.jpg

[30] Imagen recuperada de: http://www.griaulebiometrics.com/en-us/book/understanding-biometrics/evaluation/accuracy/matching/false

[31] Imagen recuperada de: https://en.wikipedia.org/wiki/Detection_error_tradeoff#/media/File:Example_of_DET_curves.png

[32] Imagen recuperada de : https://es.wikipedia.org/wiki/Curva_ROC#/media/File:ROC_space-2.png

[33] García, J. J. Sistema de autenticación biométrica de huella dactilar asistido por interfaz de voz para el control de accesos (Proyecto Fin de Carrera). Escuela Técnica Superior de Ingeniería.

[34] Reconocimiento de huellas dactilares. http://www.biometria.gov.ar/metodos-biometricos/dactilar.aspx, consultado: "Julio 2015"

[35] Sistema de Identificación mediante Huella Digital. http://fiee.uni.edu.pe/sites/default/files/index_0.pdf, consultado: "Agosto 2015"

[36] Fingerprint Recognition. https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/files/fingerprint-recognition.pdf, consultado: "Agosto 2015"

[37] Diseño de un sistema biométrico de identificación usando sensores capacitivos para huellas dactilares. http://www.scielo.org.co/scielo.php?pid=S0120-62302007000100002&script=sci_arttext, consultado: "Agosto 2015"

[38] Estudio sobre las tecnologías biométricas aplicadas a la seguridad. https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0CCkQFjABahUKEwiLurzyxovIAhXHcBoKHRK2BTg&url=https%3A%2F%2Fwww.incibe.es%2Ffile%2FtGi1Xn2W88xxCP8CLUmW_g&usg=AFQjCNGn2H8ULD03gb3GW0KsXGwibMqL4g, consultado: "Septiembre 2015"

[39] Gutiérrez J. E. (2007) Estudio de factibilidad para el control de acceso biométrico, en una empresa empleando lectores de huella digital (Proyecto Fin de Grado). Universidad de La Salle, Bogotá.

[40] Matlab. https://es.wikipedia.org/wiki/MATLAB, consultado: "Julio 2015"

ANEXO I. Configuración para obtener la librería de NBIS

Para poder utilizar las funciones proporcionadas por el algoritmo NBIS es necesario descargarse el paquete *Release 5.0.0* de la web:

http://www.nist.gov/itl/iad/ig/nigos.cfm#Releases

Una vez descargado, se descomprime la carpeta y se abre el programa Visual Studio 2013. Cuando esté abierto se carga el programa NBIS.cpp que se encuentra en la carpeta descomprimida.

Después solo hay que compilar el programa lo que generará el archivo NBIS.dll el cuál se usará como librería en la aplicación de comparación desarrollada.

Para poder usar como librería el archivo NBIS.dll, primero hay que importarla al espacio de trabajo de la aplicación de la siguiente manera:

PROJECT > Add Reference… > Browse… > Browse… > NBIS.dll > OK

Una vez importada la referencia se incluye su uso en el código de la aplicación como si se tratara de una librería más: **using Nbis;**

ANEXO II. Configuración para obtener la librería de MCC

Para poder utilizar las funciones proporcionadas por el algoritmo MCC es necesario descargarse el paquete de la web:

http://biolab.csr.unibo.it/research.asp?organize=Activities&select=&selObj=82&pathSubj=111%7C%7C8%7C%7C82&Req=&

Una vez se haya descargado el paquete, se descomprime la carpeta donde se encuentra el archivo MccSdk.dll.

Para poder usar como librería el archivo MccSdk.dll, primero hay que importarlo al espacio de trabajo de la aplicación de la siguiente manera:

PROJECT > Add Reference… > Browse… > Browse… > MccSdk.dll > OK

Una vez importada la referencia se incluye su uso en el código de la aplicación como si se tratara de una librería más: **using BioLab.Biometrics.Mcc.Sdk;**

ANEXO III. Formato de representación de minucias por NBIS y MCC

El algoritmo NBIS almacena las minucias obtenidas de cada captura con el siguiente formato [21]:

MN : MX,MY : DIR : REL : TYP : FTYP : FN : NXI, NYI : RCI : …

MN es el entero que representa el identificador de la minucia detectada.
MX es la coordenada x del píxel de la minucia detectada.
MY es la coordenada y del píxel de la minucia detectada.
DIR es la dirección de la minucia detectada.
REL es la medida de fiabilidad asignada a la minucia detectada.
TYP es el tipo de minucia detectada: bifucación (BIF), fin de cresta (RIG)...
FTYP es el tipo de característica detectada.
FN es el entero que representa el identificador del tipo de característica detectada.
NXI es la coordenada x del primer píxel de la minucia vecina detectada.
NYI es la coordenada y del primer píxel de la minucia vecina detectada.
RCI es la cuenta de crestas calculadas entre la minucia detectada y la primera minucia vecina.
… está destinado para el caso en el que se computan más de una minucia vecina, añadiendo las coordenadas x/y, además de la cuenta de crestas.

El algoritmo MCC almacena las minucias obtenidas de cada captura con el siguiente formato [24]:

imageWidth
imageHeight
imageResolution
n
x(1) y(1) ϑ(1)
x(2) y(2) ϑ(2)
...
...
...
x(n) y(n) ϑ(n)

imageWidth es el ancho de la imagen de la muestra analizada.
ImageHeight es el alto de la imagen de la muestra analizada.
ImageResolution es la resolución de la imagen de la muestra analizada.
n es el número total de minucias.
x(n) y(n) θ(n) coordenadas x e y, en píxeles, de cada minucia detectada, junto con la dirección en radianes.

ANEXO IV. Planificación y Presupuesto

En este anexo se va a llevar a cabo un desglose de las tareas realizadas a lo largo del trabajo fin de grado con el fin de estimar un presupuesto para el mismo.

A-IV. I Planificación

Se ha dividido el proyecto en distintas fases, las cuales se comentan a continuación:

Fase I. Documentación inicial

I. Estudio sobre la biometría enfocada en la identificación (15 horas)
II. Preparación de las herramientas de trabajo (7 horas)
III. Realización de pruebas y aplicaciones sencillas (35 horas)

Fase II. Desarrollo de la aplicación y obtención de resultados

I. Actividad principal (75 horas)
II. Procesado de capturas de enrol y verificación (60 horas)
III. Obtención de resultados gráficos (10 horas)
IV. Optimización y resolución de errores en código (12 horas)

Fase III. Elaboración de la memoria

I. Redacción de la memoria (70 horas)
II. Corrección y maquetación (18 horas)

En la tabla 16 se presenta un resumen del total de horas empleadas para cada tarea y en su totalidad.

Tabla 16. Desglose del total de horas empleadas para cada fase

FASES	HORAS EMPLEADAS
Documentación inicial	57
Desarrollo de la aplicación y obtención de resultados	157
Elaboración de la memoria	88
TOTAL	**302**

A-IV. II Presupuesto del Trabajo Fin de Grado

Costes materiales

Para la realización de este proyecto se han sido necesarios dos ordenadores, de altas prestaciones. Considerando un periodo de amortización de tres años y teniendo en cuenta el tiempo empleado para el trabajo los costes de material finales se exponen en la tabla 17.

Tabla 17. Costes materiales

Unidades	Concepto	Precio unitario (€)	Precio total (€)
2	Ordenador altas prestaciones	150	300
	TOTAL		**300**

Costes de personal

Este proyecto ha sido realizado por un ingeniero bajo la supervisión de un jefe y un director de proyecto. El presupuesto destinado al personal se presenta en la tabla 18.

Tabla 18. Coste de personal

OCUPACIÓN	HORAS	PRECIO/HORA	IMPORTE (€)
Director de proyecto	8	90	720
Jefe de proyecto	17	60	1020
Ingeniero	277	30	8310
TOTAL	**302**		**10050**

Coste adicional

Este trabajo se ha realizado con una base de datos previamente obtenida, los costes para su elaboración se presentan en la tabla 19.

Tabla 19. Coste adicional

CONCEPTO	PRECIO (€)
Generar una base de datos de 50 participantes	675
TOTAL	**675**

Coste total

En la tabla 20 se muestra el coste total, incluyendo los costes indirectos y el IVA.

Tabla 20. Coste total

CONCEPTO	PRECIO (€)
Costes materiales	300
Coste de personal	10050
Coste adicional	675
Costes indirectos (20%)	3200
Subtotal	14225
IVA (21%)	17212.25
TOTAL	**17212.25**

El coste total estimado para este proyecto es de DIECISIETE MIL DOSCIENTOS DOCE EUROS CON VEINTICINCO CÉNTIMOS.

Leganés, 23 de Septiembre de 2015

Sergio Sánchez